Managing Security Operations Detection Response Sans

Big Data and Data Science Engineering
Designing a HIPAA-Compliant Security Operations Center
Effective Model-Based Systems Engineering
Zero Trust Overview and Playbook Introduction
Agile Security Operations
Cybersecurity Architect's Handbook
Security Strategy
Information Assurance
Study Guide to Security Operations Centers (SOC)
Anomaly Detection as a Service
The Art of Selling IT Technology to Large Enterprises
Managing a security operations center (SOC)
NETWORKING 2011
Practical Cloud Security
Microsoft Certified: Security Operations Analyst Associate (SC-200)

Advances in Human Factors in Cybersecurity
The Practice of Network Security Monitoring
Security Architecture for Hybrid Cloud
Encyclopedia of Security Management
The Security Risk Assessment Handbook
DNS Security Management
Designing and Building Security Operations Center
CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide
Open-Source Security Operations Center (SOC)
(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide
Study Guide to SIEM (Security Information and Event Management)
Managing Digital
Internet of Things
Computer and Information Security Handbook
Commerce, Justice, Science, and Related Agencies Appropriations for 2009
Ten Strategies of a World-Class Cybersecurity Operations Center
Rational Cybersecurity for Business
Security Operations Center
Information Security Management Handbook, Fifth Edition
Information Security Management Handbook on CD-ROM, 2006 Edition

Cybersecurity Operations Handbook
The Security Risk Assessment Handbook
Practical Applications of Intelligent Systems
The CISO Playbook
Resilient Cybersecurity

MOODY AMAYA

Big Data and Data Science Engineering
Apress
In the digital age, cybersecurity is not just a necessity, but a paramount responsibility. With an ever-evolving landscape of threats, setting up and managing a Security Operations Center (SOC) has become an integral part of maintaining the security posture of organizations. "How to Manage a Security Operations Center (SOC)" is an essential guide penned by Kris Hermans, a renowned expert in the field of cybersecurity. With decades of experience in setting up and managing SOCs around the globe, Kris shares his wealth of knowledge in this comprehensive guide. In this book, you will: Understand the fundamentals of a SOC and its vital role in an organization. Learn the steps to plan, set up, and equip your SOC. Discover effective strategies for

recruiting and training a competent security team. Gain insights into managing the day-to-day operations of a SOC. Explore advanced concepts like threat intelligence, incident response, and continuous improvement for your SOC.

Designing a HIPAA-Compliant Security Operations Center

Elsevier

Do you know what weapons are used to protect against cyber warfare and what tools to use to minimize their impact? How can you gather intelligence that will allow you to configure your system to ward off attacks? Online security and privacy issues are becoming more and more significant every day, with many instances of companies and governments mishandling (or deliberately misusing) personal and financial data. Organizations need to be committed to defending their own assets and their customers' information. Designing and Building a Security Operations Center will show you how to develop the organization, infrastructure, and capabilities to protect your company and your customers effectively, efficiently, and discreetly. Written by a subject expert who has consulted on SOC implementation in both the public and private sector, Designing and Building a Security Operations Center is the go-to blueprint for cyber-defense. - Explains how to develop and build a Security Operations Center - Shows how to

gather invaluable intelligence to protect your organization - Helps you evaluate the pros and cons behind each decision during the SOC-building process

Effective Model-Based Systems Engineering

Packt Publishing Ltd

Anomaly detection has been a long-standing security approach with versatile applications, ranging from securing server programs in critical environments, to detecting insider threats in enterprises, to anti-abuse detection for online social networks. Despite the seemingly diverse application domains, anomaly detection solutions share similar technical challenges, such as how to accurately recognize various normal patterns, how to reduce false alarms, how to adapt to concept drifts, and how to minimize performance impact. They also share similar detection approaches and evaluation methods, such as feature extraction, dimension reduction, and experimental evaluation. The main purpose of this book is to help advance the real-world adoption and deployment anomaly detection technologies, by systematizing the body of existing knowledge on anomaly detection. This book is focused on data-driven anomaly detection for software, systems, and networks against advanced exploits and attacks, but also touches on a number of applications, including fraud detection and insider threats. We explain the key technical components in anomaly detection workflows, give

in-depth description of the state-of-the-art data-driven anomaly-based security solutions, and more importantly, point out promising new research directions. This book emphasizes on the need and challenges for deploying service-oriented anomaly detection in practice, where clients can outsource the detection to dedicated security providers and enjoy the protection without tending to the intricate details. *Zero Trust Overview and Playbook Introduction* CRC Press Enhance your cybersecurity and agility with this thorough playbook, featuring actionable guidance, insights, and success criteria from industry experts Key Features Get simple, clear, and practical advice for everyone from CEOs to security operations Organize your Zero Trust journey into role-by-role execution stages Integrate real-world implementation experience with global Zero Trust standards Purchase of the print or Kindle book includes a free eBook in the PDF format Book DescriptionZero Trust is cybersecurity for the digital era and cloud computing, protecting business assets anywhere on any network. By going beyond traditional network perimeter approaches to security, Zero Trust helps you keep up with ever-evolving threats. The playbook series provides simple, clear, and actionable guidance that fully answers your questions

on Zero Trust using current threats, real-world implementation experiences, and open global standards. The Zero Trust playbook series guides you with specific role-by-role actionable information for planning, executing, and operating Zero Trust from the boardroom to technical reality. This first book in the series helps you understand what Zero Trust is, why it’s important for you, and what success looks like. You’ll learn about the driving forces behind Zero Trust – security threats, digital and cloud transformations, business disruptions, business resilience, agility, and adaptability. The six-stage playbook process and real-world examples will guide you through cultural, technical, and other critical elements for success. By the end of this book, you’ll have understood how to start and run your Zero Trust journey with clarity and confidence using this one-of-a-kind series that answers the why, what, and how of Zero Trust!What you will learn Find out what Zero Trust is and what it means to you Uncover how Zero Trust helps with ransomware, breaches, and other attacks Understand which business assets to secure first Use a standards-based approach for Zero Trust See how Zero Trust links business, security, risk, and technology Use the six-stage process to guide your Zero Trust journey Transform roles and secure operations with Zero Trust Discover how the playbook guides

each role to success Who this book is forWhether you’re a business leader, security practitioner, or technology executive, this comprehensive guide to Zero Trust has something for you. This book provides practical guidance for implementing and managing a Zero Trust strategy and its impact on every role (including yours!). This is the go-to guide for everyone including board members, CEOs, CIOs, CISOs, architects, engineers, IT admins, security analysts, program managers, product owners, developers, and managers. Don't miss out on this essential resource for securing your organization against cyber threats.

Agile Security Operations Cybellium

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

Cybersecurity Architect's Handbook Elsevier

"Practical Applications of Intelligent Systems" presents selected papers from the 2013 International Conference on Intelligent Systems and Knowledge Engineering (ISKE2013). The aim of this conference is to bring together experts from different expertise areas to discuss the state-of-the-art in Intelligent Systems and Knowledge Engineering, and to present new research results and perspectives on future development. The topics in this volume include, but are not limited to: Intelligent Game, Intelligent Multimedia, Business Intelligence, Intelligent Bioinformatics Systems, Intelligent Healthcare Systems, User Interfaces and Human Computer Interaction, Knowledge-based Software Engineering, Social Issues of Knowledge Engineering, etc. The proceedings are benefit for both researchers and practitioners who want to learn more about the current practice, experience and promising new ideas in the broad area of intelligent systems and knowledge engineering. Dr. Zhenkun Wen is a Professor at the College of Computer and Software Engineering, Shenzhen University,

China. Dr. Tianrui Li is a Professor at the School of Information Science and Technology, Southwest Jiaotong University, Xi’an, China.

Security Strategy

Butterworth-Heinemann About This Book This book, "Managing Digital: Concepts and Practices", is intended to guide a practitioner through the journey of building a digital-first viewpoint and the skills needed to thrive in the digital-first world. As such, this book is a bit of an experiment for The Open Group; it isn’t structured as a traditional standard or guide. Instead, it is structured to show the key issues and skills needed at each stage of the digital journey, starting with the basics of a small digital project, eventually building to the concerns of a large enterprise. So, feel free to digest this book in stages — the section Introduction for the student is a good guide. The book is intended for both academic and industry training purposes. This book seeks to provide guidance for both new entrants into the digital workforce and experienced practitioners seeking to update their understanding on how all the various themes and components of IT management fit together in the new world. About The Open Group Press The Open Group Press is an imprint of The Open Group for advancing knowledge of information technology by publishing works from individual authors within The Open Group membership that are relevant to advancing

The Open Group mission of Boundaryless Information Flow™. The key focus of The Open Group Press is to publish high-quality monographs, as well as introductory technology books intended for the general public, and act as a complement to The Open Group Standards, Guides, and White Papers. The views and opinions expressed in this book are those of the author, and do not necessarily reflect the consensus position of The Open Group members or staff.

Information Assurance
CRC Press
This book constitutes revised selected papers from the refereed proceedings of the 5th The Global IoT Summit, GIoTS 2022, which took place in Dublin, Ireland, in June 20–23, 2022. The 33 full papers included in this book were carefully reviewed andselected from 75 submissions. They were organized in topical sections as follows: ioT enabling technologies; ioT applications, services and real implementations; ioT security, privacy and data protection; and ioT pilots, testbeds and experimentation results.
Study Guide to Security Operations Centers (SOC)
Cisco Press
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.

Anomaly Detection as a Service Springer Nature The two-volume set LNCS 6640 and 6641 constitutes the refereed proceedings of the 10th International IFIP TC 6 Networking Conference held in Valencia, Spain, in May 2011. The 64 revised full papers presented were carefully reviewed and selected from a total

of 294 submissions. The papers feature innovative research in the areas of applications and services, next generation Internet, wireless and sensor networks, and network science. The first volume includes 36 papers and is organized in topical sections on anomaly detection, content management, DTN and sensor networks, energy efficiency, mobility modeling, network science, network topology configuration, next generation Internet, and path diversity.

The Art of Selling IT Technology to Large Enterprises Springer Nature
With rapidly changing architecture and API-driven automation, cloud platforms come with unique security challenges and opportunities. In this updated second edition, you'll examine security best practices for multivendor cloud environments, whether your company plans to move legacy on-premises projects to the cloud or build a new infrastructure from the ground up. Developers, IT architects, and security professionals will learn cloud-specific techniques for securing popular cloud platforms such as Amazon Web Services, Microsoft Azure, and IBM Cloud. IBM Distinguished Engineer Chris Dotson shows you how to establish data asset management, identity and access management (IAM), vulnerability management, network security, and incident response in your cloud environment. Learn the

latest threats and challenges in the cloud security space Manage cloud providers that store or process data or deliver administrative control Learn how standard principles and concepts—such as least privilege and defense in depth—apply in the cloud Understand the critical role played by IAM in the cloud Use best tactics for detecting, responding, and recovering from the most common security incidents Manage various types of vulnerabilities, especially those common in multicloud or hybrid cloud architectures Examine privileged access management in cloud environments

Managing a security operations center (SOC) CRC Press

Develop a comprehensive plan for building a HIPAA-compliant security operations center, designed to detect and respond to an increasing number of healthcare data breaches and events. Using risk analysis, assessment, and management data combined with knowledge of cybersecurity program maturity, this book gives you the tools you need to operationalize threat intelligence, vulnerability management, security monitoring, and incident response processes to effectively meet the challenges presented by healthcare's current threats. Healthcare entities are bombarded with data. Threat intelligence feeds, news updates, and messages come rapidly and in many forms such as email, podcasts, and more. New vulnerabilities are found

every day in applications, operating systems, and databases while older vulnerabilities remain exploitable. Add in the number of dashboards, alerts, and data points each information security tool provides and security teams find themselves swimming in oceans of data and unsure where to focus their energy. There is an urgent need to have a cohesive plan in place to cut through the noise and face these threats. Cybersecurity operations do not require expensive tools or large capital investments. There are ways to capture the necessary data. Teams protecting data and supporting HIPAA compliance can do this. All that's required is a plan—which author Eric Thompson provides in this book. What You Will Learn Know what threat intelligence is and how you can make it useful Understand how effective vulnerability management extends beyond the risk scores provided by vendors Develop continuous monitoring on a budget Ensure that incident response is appropriate Help healthcare organizations comply with HIPAA Who This Book Is For Cybersecurity, privacy, and compliance professionals working for organizations responsible for creating, maintaining, storing, and protecting patient information.

NETWORKING 2011 Packt Publishing Ltd

Welcome to the forefront of knowledge with Cybellium, your trusted partner in mastering the cutting-edge fields of IT, Artificial Intelligence,

Cyber Security, Business, Economics and Science. Designed for professionals, students, and enthusiasts alike, our comprehensive books empower you to stay ahead in a rapidly evolving digital world. * Expert Insights: Our books provide deep, actionable insights that bridge the gap between theory and practical application. * Up-to-Date Content: Stay current with the latest advancements, trends, and best practices in IT, Al, Cybersecurity, Business, Economics and Science. Each guide is regularly updated to reflect the newest developments and challenges. * Comprehensive Coverage: Whether you're a beginner or an advanced learner, Cybellium books cover a wide range of topics, from foundational principles to specialized knowledge, tailored to your level of expertise. Become part of a global network of learners and professionals who trust Cybellium to guide their educational journey. www.cybellium.com

Practical Cloud Security John Wiley & Sons

Build a robust cybersecurity program that adapts to the constantly evolving threat landscape Key Features Gain a deep understanding of the current state of cybersecurity, including insights into the latest threats such as Ransomware and AI Lay the foundation of your cybersecurity program with a comprehensive approach allowing for continuous maturity Equip

yourself and your organizations with the knowledge and strategies to build and manage effective cybersecurity strategies Book DescriptionBuilding a Comprehensive Cybersecurity Program addresses the current challenges and knowledge gaps in cybersecurity, empowering individuals and organizations to navigate the digital landscape securely and effectively. Readers will gain insights into the current state of the cybersecurity landscape, understanding the evolving threats and the challenges posed by skill shortages in the field. This book emphasizes the importance of prioritizing well-being within the cybersecurity profession, addressing a concern often overlooked in the industry. You will construct a cybersecurity program that encompasses architecture, identity and access management, security operations, vulnerability management, vendor risk management, and cybersecurity awareness. It dives deep into managing Operational Technology (OT) and the Internet of Things (IoT), equipping readers with the knowledge and strategies to secure these critical areas. You will also explore the critical components of governance, risk, and compliance (GRC) within cybersecurity programs, focusing on the oversight and management of these functions. This book provides practical insights, strategies, and knowledge to help

organizations build and enhance their cybersecurity programs, ultimately safeguarding against evolving threats in today's digital landscape.What you will learn Build and define a cybersecurity program foundation Discover the importance of why an architecture program is needed within cybersecurity Learn the importance of Zero Trust Architecture Learn what modern identity is and how to achieve it Review of the importance of why a Governance program is needed Build a comprehensive user awareness, training, and testing program for your users Review what is involved in a mature Security Operations Center Gain a thorough understanding of everything involved with regulatory and compliance Who this book is for This book is geared towards the top leaders within an organization, C-Level, CISO, and Directors who run the cybersecurity program as well as management, architects, engineers and analysts who help run a cybersecurity program. Basic knowledge of Cybersecurity and its concepts will be helpful. *Microsoft Certified: Security Operations Analyst Associate (SC-200)* Cybellium The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments provides detailed insight into precisely how to conduct an information security risk assessment. Designed for security professionals and their

customers who want a more in-depth understanding of the risk assessment process, this volume contains real-wor
Advances in Human Factors in Cybersecurity
CRC Press
This textbook presents a proven, mature Model-Based Systems Engineering (MBSE) methodology that has delivered success in a wide range of system and enterprise programs. The authors introduce MBSE as the state of the practice in the vital Systems Engineering discipline that manages complexity and integrates technologies and design approaches to achieve effective, affordable, and balanced system solutions to the needs of a customer organization and its personnel. The book begins with a summary of the background and nature of MBSE. It summarizes the theory behind Object-Oriented Design applied to complex system architectures. It then walks through the phases of the MBSE methodology, using system examples to illustrate key points. Subsequent chapters broaden the application of MBSE in Service-Oriented Architectures (SOA), real-time systems, cybersecurity, networked enterprises, system simulations, and prototyping. The vital subject of system and architecture governance completes the discussion. The book features exercises at the end of each chapter intended to help readers/students focus on key points, as well as extensive appendices that furnish

additional detail in particular areas. The self-contained text is ideal for students in a range of courses in systems architecture and MBSE as well as for practitioners seeking a highly practical presentation of MBSE principles and techniques.
The Practice of Network Security Monitoring
Apress
Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.
Security Architecture for Hybrid Cloud Springer Nature
Trust the best-selling Official Cert Guide series from Cisco Press to help you learn, prepare, and practice for the CCNP and CCIE Security Core SCOR 350-701 exam. Well regarded for its level of detail, study plans, assessment features, and

challenging review questions and exercises, CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide, Second Edition helps you master the concepts and techniques that ensure your exam success and is the only self-study resource approved by Cisco. Expert author Omar Santos shares preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. This complete study package includes A test-preparation routine proven to help you pass the exam Do I Know This Already? quizzes, which let you decide how much time you need to spend on each section Exam Topic lists that make referencing easy Chapter-ending exercises, which help you drill on key concepts you must know thoroughly The powerful Pearson Test Prep Practice Test software, complete with hundreds of well-reviewed, exam-realistic questions, customization options, and detailed performance reports A final preparation chapter, which guides you through tools and resources to help you craft your review and test-taking strategies Study plan suggestions and templates to help you organize and optimize your study time Content Update Program: This fully updated second edition includes the latest topics and additional information covering changes to the latest CCNP and CCIE Security Core SCOR 350-701 exam. Visit ciscopress.com/newcerts for information on annual

digital updates for this book that align to Cisco exam blueprint version changes. This official study guide helps you master all the topics on the CCNP and CCIE Security Core SCOR 350-701 exam, including Network security Cloud security Content security Endpoint protection and detection Secure network access Visibility and enforcement Companion Website: The companion website contains more than 200 unique practice exam questions, practice exercises, and a study planner Pearson Test Prep online system requirements: Browsers: Chrome version 73 and above, Safari version 12 and above, Microsoft Edge 44 and above. Devices: Desktop and laptop computers, tablets running Android v8.0 and above or iPadOS v13 and above, smartphones running Android v8.0 and above or iOS v13 and above with a minimum screen size of 4.7”. Internet access required. Pearson Test Prep offline system requirements: Windows 11, Windows 10, Windows 8.1; Microsoft .NET Framework 4.5 Client; Pentium-class 1 GHz processor (or equivalent); 512 MB RAM; 650 MB disk space plus 50 MB for each downloaded practice exam; access to the Internet to register and download exam databases Also available from Cisco Press for CCNP Advanced Routing study is the CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide Premium Edition eBook and Practice Test, Second Edition This digital-only certification

preparation product combines an eBook with enhanced Pearson Test Prep Practice Test. This integrated learning package Enables you to focus on individual topic areas or take complete, timed exams Includes direct links from each question to detailed tutorials to help you understand the concepts behind the questions Provides unique sets of exam-realistic practice questions Tracks your performance and provides feedback on a module-by-module basis, laying out a complete assessment of your knowledge to help you focus your study where it is needed most

Encyclopedia of Security Management

Cybellium Ltd

The need for information security management has never been greater. With constantly changing technology, external intrusions, and internal thefts of data, information security officers face threats at every turn. The Information Security Management Handbook on CD-ROM, 2006 Edition is now available. Containing the complete contents of the Information Security Management Handbook, this is a resource that is portable, linked and searchable by keyword. In addition to an electronic version of the most comprehensive resource for information security management, this CD-ROM contains an extra volume's worth of information that is not found anywhere else, including chapters from other security and networking books that have never appeared in

the print editions. Exportable text and hard copies are available at the click of a mouse. The Handbook's numerous authors present the ten domains of the Information Security Common Body of Knowledge (CBK) ®. The CD-ROM serves as an everyday reference for information security practitioners and an important tool for any one preparing for the Certified Information System Security Professional (CISSP) ® examination. New content to this Edition: Sensitive/Critical Data Access Controls Role-Based Access Control Smartcards A Guide to Evaluating Tokens Identity Management-Benefits and Challenges An Examination of Firewall Architectures The Five "W's" and Designing a Secure Identity Based Self-Defending Network Maintaining Network Security-Availability via Intelligent Agents PBX Firewalls: Closing the Back Door Voice over WLAN Spam Wars: How to Deal with Junk E-Mail Auditing the Telephony System: Defenses against Communications Security Breaches and Toll Fraud The "Controls" Matrix Information Security Governance

The Security Risk Assessment Handbook

CRC Press

Cybersecurity Operations Handbook is the first book for daily operations teams who install, operate and maintain a range of security technologies to protect corporate infrastructure. Written by experts in security operations, this book provides extensive

guidance on almost all aspects of daily operational security, asset protection, integrity management, availability methodology, incident response and other issues that operational teams need to know to properly run security products and services in a live environment. Provides a master document on Mandatory FCC Best Practices and complete coverage of all critical operational procedures for meeting Homeland Security requirements.·First book written for daily operations teams·Guidance on almost all aspects of daily operational security, asset protection, integrity management·Critical information for compliance with Homeland Security