The Cert Guide To Insider Threats How To Prevent Detect And Respond To Information Technology Crimes Theft Sabotage Fraud Sei Series In Software Engineering Hardcover

The CERT Guide to Insider Threats The CERT Guide to Insider Threats Insider Threats Insider Threats in Cyber Security Insider Threat Insider Threat Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft Managing the Insider Threat Inside Jobs The Insider Threat Enemy at the Water Cooler Data Protection from Insider Threats Insider Attack and Cyber Security Protecting Your Business from Insider Threats in Seven Effective Steps The Insider Threat Big Data Analytics with Applications in Insider Threat Detection The Insider Threat Insider Threats Insider Computer Fraud Insider Threats in Cyber Security Managing the Insider Threat Hands-On Cybersecurity for Finance Insider Threat Cybersecurity Education for Awareness and Compliance Insider Threat Human Aspects of Information Security, Privacy, and Trust Insider Threat Program Human Aspects of Information Security, Privacy, and Trust Network Security Bible Threat Assessment Mastering Defensive Security Cyber Insider Threat: Trustworthiness in Virtual Organizations Workplace Violence Prevention and Response Guideline Human-Computer Interaction and Cybersecurity Handbook Insider Threats Social, Cultural, and Behavioral Modeling Privileged Attack Vectors Research Anthology on Business Aspects of Cybersecurity The Insider Threat Embedded Enemy

Eventually, you will entirely discover a extra experience and carrying out by spending more cash. yet when? accomplish you agree to that you require to get those every needs later having significantly cash? Why dont you attempt to get something basic in the beginning? Thats something that will guide you to comprehend even more re the globe, experience, some places, subsequently history, amusement, and a lot more?

It is your totally own period to accomplish reviewing habit. in the midst of guides you could enjoy now is The Cert Guide To Insider Threats How To Prevent Detect And Respond To Information Technology Crimes Theft Sabotage Fraud Sei Series In Software Engineering Hardcover below.

Cybersecurity Education for Awareness and Compliance Nov 09 2020 Understanding cybersecurity principles and practices is vital to all users of IT systems and services, and is particularly relevant in an organizational setting where the lack of security awareness and compliance amongst staff is the root cause of many incidents and breaches. If these are to be addressed, there needs to be adequate support and provision for related training and education in order to ensure that staff know what is expected of them and have the necessary skills to follow through. Cybersecurity Education for Awareness and Compliance explores frameworks and models for teaching cybersecurity literacy in order to deliver effective training and compliance to organizational staff so that they have a clear understanding of what security education is, the elements required to achieve it, and the means by which to link it to the wider goal of good security behavior. Split across four thematic sections (considering the needs of users, organizations, academia, and the profession, respectively), the chapters will collectively identify and address the multiple perspectives from which action is required. This book is ideally designed for IT consultants and specialist staff including chief information security officers, managers, trainers, and organizations.

Managing the Insider Threat Mar 26 2022 An adversary who attacks an organization from within can prove fatal to the organization and is generally impervious to conventional defenses. Drawn from the findings of an award-winning thesis, Managing the Insider Threat: No Dark Corners is the first comprehensive resource to use social science research to explain why traditional methods fail aga

Insider Threats in Cyber Security Jul 30 2022 Insider Threats in Cyber Security is a cutting edge text presenting IT and non-IT facets of insider threats together. This volume brings together a critical mass of well-established worldwide researchers, and provides a unique multidisciplinary overview. Monica van Huystee, Senior Policy Advisor at MCI, Ontario, Canada comments "The book will be a must read, so of course I'll need a copy." Insider Threats in Cyber Security covers all aspects of insider threats, from motivation to mitigation. It includes how to monitor insider threats (and what to monitor for), how to mitigate insider threats, and related topics and case studies. Insider Threats in Cyber Security is intended for a professional audience composed of the military, *government policy makers and banking; financing companies focusing on the Secure Cyberspace industry. This book is also suitable for advanced-level students and researchers in computer science as a secondary text or reference book.*

Data Protection from Insider Threats Nov 21 2021 As data represent a key asset for today's organizations, the problem of how to protect this data from theft and misuse is at the forefront of these organizations' minds. Even though today several data security techniques are available to protect data and computing infrastructures, many such techniques -- such as firewalls and network security tools -- are unable to protect data from attacks posed by those working on an organization's "inside." These "insiders" usually have authorized access to relevant information systems, making it extremely challenging to block the misuse of information while still allowing them to do their jobs. This book discusses several techniques that can provide effective protection against attacks posed by people working on the inside of an organization. Chapter One introduces the notion of insider threat and reports some data about data breaches due to insider threats. Chapter Two covers authentication and access control techniques, and Chapter Three shows how these general security techniques can be extended and used in the context of protection from insider threats. Chapter Four addresses anomaly detection techniques that are used to determine anomalies in data accesses by insiders. These anomalies are often indicative of potential insider data attacks and therefore play an important role in protection from these attacks. Security information and event management (SIEM) tools and fine-grained auditing are discussed in Chapter Five. These tools aim at collecting, analyzing, and correlating -- in real-time -- any information and event that may be relevant for the security of an organization. As such, they can be a key element in finding a solution to such undesirable insider threats. Chapter Six goes on to provide a survey of techniques for separation-of-duty (SoD). SoD is an important principle that, when implemented in systems and tools, can strengthen data protection from malicious insiders. However, to date, very few approaches have been proposed for implementing SoD in systems. In Chapter Seven, a short survey of a commercial product is presented, which provides different techniques for protection from malicious users with system privileges -- such as a DBA in database management systems. Finally, in Chapter Eight, the book concludes with a few remarks and additional research directions. Table of Contents: Introduction / Authentication / Access Control / Anomaly Detection / Security Information and Event Management and Auditing / Separation of Duty / Case Study: Oracle Database Vault / Conclusion

Mastering Defensive Security Apr 02 2020 An immersive learning experience enhanced with technical, hands-on labs to understand the concepts, methods, tools, platforms, and systems required to master the art of cybersecurity Key FeaturesGet hold of the best defensive security strategies and toolsDevelop a defensive security strategy at an enterprise levelGet hands-on with advanced cybersecurity threat detection, including XSS, SQL injections, brute forcing web applications, and moreBook Description Every organization has its own data and digital assets that need to be protected against an ever-growing threat landscape that compromises the availability, integrity, and confidentiality of crucial data. Therefore, it is important to train professionals in the latest defensive security skills and tools to secure them. Mastering Defensive Security provides you with in-depth knowledge of the latest cybersecurity threats along with the best tools and techniques needed to keep your infrastructure secure. The book begins by establishing a strong foundation of cybersecurity concepts and advances to explore the latest security technologies such as Wireshark, Damn Vulnerable Web App (DVWA), Burp Suite, OpenVAS, and Nmap, hardware threats such as a weaponized Raspberry Pi, and hardening techniques for Unix, Windows, web applications, and cloud infrastructures. As you make progress through the chapters, you'll get to grips with several advanced techniques such as malware analysis, security automation, computer forensics, and vulnerability assessment, which will help you to leverage pentesting for security. By the end of this book, you'll have become familiar with creating your own defensive security tools using IoT devices and developed advanced defensive security skills. What you will learnBecome well versed with concepts related to defensive securityDiscover strategies and tools to secure the most vulnerable factor – the userGet hands-on experience using and configuring the best security toolsUnderstand how to apply hardening techniques in Windows and Unix environmentsLeverage malware analysis and forensics to enhance your security strategySecure Internet of Things (IoT) implementationsEnhance the security of web applications and cloud deploymentsWho this book is for This book is for all IT professionals who want to take their first steps into the world of defensive security; from system admins and programmers to data analysts and data scientists with an interest in security. Experienced cybersecurity professionals working on broadening their knowledge and keeping up to date with the latest defensive developments will also find plenty of useful information in this book. You'll need a basic understanding of networking, IT, servers, virtualization, and cloud platforms before you get started with this book.

Protecting Your Business from Insider Threats in Seven Effective Steps Sep 19 2021 How resilient is your *organisation to someone from within behaving in a way that places your organisation at risk?Every organisation wants to believe that their employees are beyond reproach, trustworthy and loyal. But are they?An insider can pose a massive threat to your business due to their knowledge of, and access to, the employer's systems and information. They can easily bypass physical and electronic security measures through legitimate means.Insiders have knowledge of where your valuable assets are. They will know how, when and where to attack and how to cover their tracks. Insiders can target the asset directly and do not need to overcome the barriers which face external hackers. But not all insiders are malicious. Most incidents are the result of human error.Verizon 2015 Data Breach Investigation Report interestingly stated that 90% of all incidents are people. Whether it's goofing up, getting infected, behaving badly, or losing stuff.Your biggest threat are your insiders, but you are just now aware of it.This book is to present to you, show you, convince you of why your organisation is at risk and what the seven steps that you can take to mitigate insider threat right now*

Insider Attack and Cyber Security Oct 21 2021 This book defines the nature and scope of insider problems as viewed by the financial industry. This edited volume is based on the first workshop on Insider Attack and Cyber Security, IACS 2007. The workshop was a joint effort from the Information Security Departments of Columbia University and Dartmouth College. The book sets an agenda for an ongoing research initiative to solve one of the most vexing problems encountered in security, and a range of topics from critical IT infrastructure to insider threats. In some ways, the insider problem is the ultimate security problem.

Insider Computer Fraud Apr 14 2021 An organization’s employees are often more intimate with its computer system than anyone else. Many also have access to sensitive information regarding the company and its customers. This makes employees prime candidates for sabotaging a system if they become disgruntled or for selling privileged information if they become greedy. Insider Computer Fraud: An In-depth Framework for Detecting and Defending against Insider IT Attacks presents the methods, safeguards, and techniques that help protect an organization from insider computer fraud. Drawing from the author’s vast experience assessing the adequacy of IT security for the banking and securities industries, the book presents a practical framework for identifying, measuring, monitoring, and controlling the risks associated with insider threats. It not only provides an analysis of application or system-related risks, it demonstrates the interrelationships that exist between an application and the IT infrastructure components it uses to transmit, process, and store sensitive data. The author also examines the symbiotic relationship between the risks, controls, threats, and action plans that should be deployed to enhance the overall information security governance processes. Increasing the awareness and understanding necessary to effectively manage the risks and controls associated with an insider threat, this book is an invaluable resource for those interested in attaining sound and best practices over the risk management process.

Insider Threat Jun 28 2022 Insider Threat: Detection, Mitigation, Deterrence and Prevention presents a set of solutions to address the increase in cases of insider threat. This includes espionage, embezzlement, sabotage, fraud, intellectual property theft, and research and development theft from current or former employees. This book outlines a step-by-step path for developing an insider threat program within any organization, focusing on management and employee engagement, as well as ethical, legal, and privacy concerns. In addition, it includes tactics on how to collect, correlate, and visualize potential risk indicators into a seamless system for protecting an organization’s critical assets from malicious, complacent, and ignorant insiders. Insider Threat presents robust mitigation strategies that will interrupt the forward motion of a potential insider who intends to do harm to a company or its employees, as well as an understanding of supply chain risk and cyber security, as they relate to insider threat. Offers an ideal resource for executives and managers who want the latest information available on protecting their organization’s assets from this growing threat Shows how departments across an entire organization can bring disparate, but related, information together to promote the early identification of insider threats Provides an in-depth explanation of mitigating supply chain risk Outlines progressive approaches to cyber security

Workplace Violence Prevention and Response Guideline Jan 30 2020

Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft Apr 26 2022 The Secret Service, FBI, NSA, CERT (Computer Emergency Response Team) and George Washington University have all identified “Insider Threats as one of the most significant challenges facing IT, security, law enforcement, and intelligence professionals today. This book will teach IT professional and law enforcement officials about the dangers posed by insiders to their IT infrastructure and how to mitigate these risks by designing and implementing secure IT systems as well as security and human resource policies. The book will begin by identifying the types of insiders who are most likely to pose a threat. Next, the reader will learn about the variety of tools and attacks used by insiders to commit their crimes including: encryption, steganography, and social engineering. The book will then *specifically address the dangers faced by corporations and government agencies. Finally, the reader will learn how to design effective security systems to prevent insider attacks and how to investigate insider security breeches that do occur. Throughout the book, the authors will use their backgrounds in the CIA to analyze several, high-profile cases involving insider threats. * Tackles one of the most significant challenges facing IT, security, law enforcement, and intelligence professionals today * Both co-authors worked for several years at the CIA, and they use this experience to analyze several high-profile cases involving insider threat attacks * Despite the frequency and harm caused by insider attacks, there are no competing books on this topic.books on this topic*

Insider Threats May 16 2021 An information system may be regarded as an organized set of resources, both technological and human. Security should take this specificity into consideration in order to ensure an overall security of information systems. The security of information systems is usually tackled in a technological perspective. This book proposes to focus not only on information systems' security in a technological perspective, but also in a human, managerial and organizational perspective.

The Insider Threat Jan 24 2022 This book provides emergent knowledge relating to physical, cyber, and human risk mitigation in a practical and readable approach for the corporate environment. It presents and discusses practical applications of risk management techniques along with useable practical policy change options. This practical organizational security management approach examines multiple aspects of security to protect against physical, cyber, and human risk. A practical more tactical focus includes managing vulnerabilities and applying countermeasures. The book guides readers to a greater depth of understanding and action-oriented options.

Network Security Bible Jun 04 2020 The comprehensive A-to-Z guide on network security, fully revised and updated Network security is constantly evolving, and this comprehensive guide has been thoroughly updated to cover the newest developments. If you are responsible for network security, this is the reference you need at your side. Covering new techniques, technology, and methods for approaching security, it also examines new trends and best practices being used by many organizations. The revised Network Security Bible complements the Cisco Academy course instruction in networking security. Covers all core areas of network security and how they interrelate Fully revised to address new techniques, technology, and methods for securing an enterprise worldwide Examines new trends and best practices in use by organizations to secure their enterprises Features additional chapters on areas related to data protection/correlation and forensics Includes cutting-edge topics such as integrated cybersecurity and sections on Security Landscape, with chapters on validating security, data protection, forensics, and attacks and threats If you need to get up to date or stay current on network security, Network Security Bible, 2nd Edition covers everything you need to know.

Insider Threats Nov 29 2019 This book outlines courses of action that organizational leaders and HR professionals can take to minimize the risks associated with insider threats and to minimize the losses when these threats materialize. In addition to examining technical safeguards, it shows business leaders ways to continually assess employee performance and behaviors with an eye toward minimizing their organization's vulnerability to insider threats.

Threat Assessment May 04 2020 Detailed “how to's” of threat assessment—from the initial contact to the sharing of results! Risk management can be an organizational nightmare, but it is an essential part of your operations. Recent events have shown us that organizations need to know how to respond swiftly and effectively in emergencies and that companies need to protect their employees from internal and external threats. This book provides you with the tools you need to protect both your employees and yourself from a variety of threats. Threat Assessment: A Risk Management Approach examines the factors that human resource, security, legal, and behavioral professionals need to understand in work violence and threat situations that disrupt the working environment, revealing the best ways to reduce risk and manage emergencies. It includes case studies and hypothetical examples that show recommended practices in action and provides detailed interviewing methods that can increase the efficiency of current strategies. Helpful appendices provide sample forms for identification cards, stay-away letters, workplace behavior improvement plans for problem employees, questions for health care providers, and announcements for employees regarding security changes. An extensive bibliography points the way to other useful material on this subject. Threat Assessment: A Risk Management Approach explores: the role of the multidisciplinary threat management team corporate liaisons with law enforcement agencies cyberthreats and stalking insider threats category classification of offending behaviors Risk management is a constantly evolving field, and Threat Assessment provides you with access to the latest updates. Staying up-to-date on risk management innovations will help you increase corporate sensitivity to possible threats and provide the safest possible working environment to your employees. The authors of Threat Assessment are seasoned professionals with extensive experience in risk management. You can learn from their expertise and adapt it to your situation, improving workplace safety and contributing to security in your own community.

Social, Cultural, and Behavioral Modeling Oct 28 2019 This book constitutes the proceedings of the 13th International Conference on Social, Cultural, and Behavioral Modeling, SBP-BRiMS 2020, which was planned to take place in Washington, DC, USA. Due to the COVID-19 pandemic the conference was held online during October 18–21, 2020. The 33 full papers presented in this volume were carefully reviewed and selected from 66 submissions. A wide number of disciplines are represented including computer science, psychology, sociology, communication science, public health, bioinformatics, political science, and organizational science. Numerous types of computational methods are used, such as machine learning, language technology, social network analysis and visualization, agent-based simulation, and statistics.

The CERT Guide to Insider Threats Oct 01 2022 Wikileaks recent data exposures demonstrate the danger now posed by insiders, who can often bypass physical and technical security measures designed to prevent unauthorized access. The insider threat team at CERT helps readers systematically identify, prevent, detect, and mitigate threats.

Insider Threat Program Aug 07 2020 Company insiders are responsible for 90% of security incidents. Of these, 29% are due to deliberate and malicious actions, and 71% result from unintentional actions. Unfortunately, today's piecemeal and ad hoc approach is simply not working. You need a holistic Insider Threat Management Program (ITMP) to effectively manage these threats and reduce the risk to your corporate assets.

Insider Threat May 28 2022 Every type of organization is vulnerable to insider abuse, errors, and malicious attacks: Grant anyone access to a system and you automatically introduce a vulnerability. Insiders can be current or former employees, contractors, or other business partners who have been granted authorized access to networks, systems, or data, and all of them can bypass security measures through legitimate means. Insider Threat – A Guide to Understanding, Detecting, and Defending Against the Enemy from Within shows how a security culture based on international best practice can help mitigate the insider threat, providing short-term quick fixes and long-term solutions that can be applied as part of an effective insider threat program. Read this book to learn the seven organizational characteristics common to insider threat victims; the ten stages of a malicious attack; the ten steps of a successful insider threat program; and the construction of a three-tier security culture, encompassing artefacts, values, and shared assumptions. Perhaps most importantly, it also sets out what not to do, listing a set of worst practices that should be avoided. About the author Dr Julie Mehan is the founder and president of JEMStone Strategies and a principal in a strategic consulting firm in Virginia. She has delivered cybersecurity and related privacy services to senior commercial, Department of Defense, and federal government clients. Dr Mehan is also an associate professor at the University of Maryland University College, specializing in courses in cybersecurity, cyberterror, IT in organizations, and ethics in an Internet society

Human Aspects of Information Security, Privacy, and Trust Jul 06 2020 This book constitutes the proceedings of the Second International Conference on Human Aspects of Information Security, Privacy, and Trust, HAS 2014, held as part of HCI International 2014 which took place in Heraklion, Crete, Greece, in June 2014 and incorporated 14 conferences which similar thematic areas. HCII 2014 received a total of 4766 submissions, of which 1476 papers and 220 posters were accepted for publication after a careful reviewing process. These papers address the latest research and development efforts and highlight the human aspects of design and use of computing systems. The papers thoroughly cover the entire field of Human-Computer Interaction, addressing major advances in knowledge and effective use of computers in a variety of application areas. The 38 papers presented in the HAS 2014 proceedings are organized in topical sections named: usable security; authentication and passwords; security policy and awareness; human behaviour in cyber security and privacy issues.

Insider Threat Dec 11 2020 Insider Threat - A Guide to Understanding, Detecting, and Defending Against the Enemy from Withinlooks beyond perimeter protection tools, and shows how a security culture based on international best practice can help mitigate the insider threat to your security. It also provides some short-term quick fixes that can be applied as your organizations builds an effective insider threat programme. Read this book to learn: .The seven organizational characteristics common to insider threat victims. .The ten stages of a malicious attack. .The ten steps of a successful insider threat programme. .How to construct a three-tier security culture, encompassing artefacts, values and shared assumptions. Insider Threatdetails the measures that organizations can implement to ensure high-impact quick wins, mapping appropriate security controls from the ISO 27001, ISO 27002, and NIST SP 800-53 standards to the following points, and more: .Risk mitigation and the eight steps of a risk assessment .The importance of training and awareness, and conducting staff background screening .Monitoring and auditing the activities of general and privileged users, and quickly responding to suspicious behaviors .Metrics to measure insider threat behavior and mitigation .The challenge of external or temporary insiders (such as consultants, support contractors, partners, service providers, temporary employees) .Layering physical and digital defenses to provide defense in depth .The importance of conducting regular *penetration testing to evaluate security controls .Limiting, monitoring and controlling remote access and mobile device use .Ensuring supply-chain security .Maintaining an incident management capability It also sets out what not to do, listing a set of worst practices that should be avoided."*

Embedded Enemy Jun 24 2019 Embedded Enemy is the true story of the unprecedented deadly attack against the men and women of Headquarters and Headquarters Company First Brigade, 101st Airborne Division. Shortly after deploying for the war in Iraq, the Bastogne Brigade was staged at Camp Pennsylvania in Kuwait where they prepared for combat against Saddam Hussein's Baathist regime. During the eerie, pitch-black, early morning hours of 23 March 2003, a fellow American soldier, Sergeant Hasan Akbar, executed the unthinkable and unlikeliest of scenarios by throwing hand grenades into his Chain of Command's tents. He then followed up with small-arms fire while his Commanding Officers slept in preparation for war.The wicked aftermath killed two officers and wounded 12 others. Six soldiers were evacuated, never to return-all were vital to the unit's arduous mission. Despite the tragic deaths in the most unfathomable way, the Bastogne Brigade received movement orders to cross the border into Iraq just 48 hours after the attack.This story is about how the soldiers bonded together to rescue, treat, and evacuate their brothers at arms in the midst of the shadows of darkness, massive explosions, rapid gun fire, suffocating smoke, body ripping shrapnel, and complete and total chaos and confusion. All of this was accomplished while simultaneously searching for a ruthless killer that had taken the same oath to defend the Constitution of the United States against foreign enemies. Little did they realize they would meet the most improbable of adversaries-one of their very own-an "Embedded Enemy."This event shocked the Armed Forces, America, and people around the world. It forced everyone to more carefully consider whom we really trust and to begin to digest the idea that threats to our personal safety might now come "from the inside."

Cyber Insider Threat: Trustworthiness in Virtual Organizations Mar 02 2020 This study examines human trustworthiness as a key component in countering insider threats. The term insider threat refers to situations where a critical member of an organization behaves against the interests of the organization, in an illegal and/or unethical manner. This study adopts the attribution of human-observed changes in behavior as analogous to a group of "sensors" on a computer network. Using online team-based games, this study re-creates realistic insider threat situations in which human sensors have the opportunity to observe changes in the behavior of a focal individual. The intellectual merit of this sociotechnical study lies in its capability to tackle complex insider threat problems by adopting a social psychological theory on predicting human trustworthiness in a virtual collaborative environment. The study contributes to a theoretical framework of trustworthiness attribution in geographically dispersed virtual organizations. The broader impact of this study may lead to the development of sociotechnical systems: an intelligence-based sensor system that analyzes trustworthiness based on human virtual interactions, in an attempt to predict malfeasance.

Human Aspects of Information Security, Privacy, and Trust Sep 07 2020 This book constitutes the proceedings of the Third International Conference on Human Aspects of Information Security, Privacy, and Trust, HAS 2015, held as part of the 17th International Conference on Human-Computer Interaction, HCII 2015, held in Los Angeles, CA, USA, in August 2015 and received a total of 4843 submissions, of which 1462 papers and 246 posters were accepted for publication after a careful reviewing process. These papers address the latest research and development efforts and highlight the human aspects of design and use of computing systems. The papers thoroughly cover the entire field of Human-Computer Interaction, addressing major advances in knowledge and effective use of computers in a variety of application areas. The 62 papers presented in the HAS 2015 proceedings are organized in topical sections as follows: authentication, cybersecurity, privacy, security, and user behavior, security in social media and smart technologies, and security technologies.

The Insider Threat Aug 19 2021 In the eighth action-packed thriller in the New York Times bestselling Pike Logan series, ISIS, the most maniacal terrorist organization the modern world has ever seen, is poised to make their most audacious strike yet. The United States has anticipated and averted countless attacks from terrorist groups—thanks in large part to the extralegal counterterrorist unit known as the Taskforce. But in The Insider Threat, a much more insidious evil is about to shatter the false sense of safety surrounding civilized nations. While world powers combat ISIS on the battlefield, a different threat is set in motion by the group—one that can't be defeated by an airstrike. Off the radar of every Western intelligence organization, able to penetrate America or any European state, they intend to commit an act of unimaginable barbarity. Only Pike Logan and the Taskforce stand in the way of an attack no one anticipates, a grand deception that will wreak unthinkable chaos and reverberate throughout the Western world.

Research Anthology on Business Aspects of Cybersecurity Aug 26 2019 "This reference book considers all emerging aspects of cybersecurity in the business sector including frameworks, models, best practices, and emerging areas of interest, discussing items such as audits and risk assessments that businesses can conduct to *ensure the security of their systems, training and awareness initiatives for staff that promotes a security culture and software and systems that can be used to secure and manage cybersecurity threats"--*

The CERT Guide to Insider Threats Nov 02 2022 Since 2001, the CERT® Insider Threat Center at Carnegie Mellon University's Software Engineering Institute (SEI) has collected and analyzed information about more than seven hundred insider cyber crimes, ranging from national security espionage to theft of trade secrets. The CERT® Guide to Insider Threats describes CERT's findings in practical terms, offering specific guidance and countermeasures that can be immediately applied by executives, managers, security officers, and operational staff within any private, government, or military organization. The authors systematically address attacks by all types of malicious insiders, including current and former employees, contractors, business partners, outsourcers, and even cloud-computing vendors. They cover all major types of insider cyber crime: IT sabotage, intellectual property theft, and fraud. For each, they present a crime profile describing how the crime tends to evolve over time, as well as motivations, attack methods, organizational issues, and precursor warnings that could have helped the organization prevent the incident or detect it earlier. Beyond identifying crucial patterns of suspicious behavior, the authors present concrete defensive measures for protecting both systems and data. This book also conveys the big picture of the insider threat problem over time: the complex interactions and unintended consequences of existing policies, practices, technology, insider mindsets, and organizational culture. Most important, it offers actionable recommendations for the entire organization, from executive management and board members to IT, data owners, HR, and legal departments. With this book, you will find out how to Identify hidden signs of insider IT sabotage, theft of sensitive information, and fraud Recognize insider threats throughout the software development life cycle Use advanced threat controls to resist attacks by both technical and nontechnical insiders Increase the effectiveness of existing technical security tools by enhancing rules, configurations, and associated business processes Prepare for unusual insider attacks, including attacks linked to organized crime or the Internet underground By implementing this book's security practices, you will be incorporating protection mechanisms designed to resist the vast majority of malicious insider attacks.

Insider Threat Oct 09 2020 Insider Threat: Detection, Mitigation, Deterrence and Prevention presents a set of solutions to address the increase in cases of insider threat. This includes espionage, embezzlement, sabotage, fraud, intellectual property theft, and research and development theft from current or former employees. This book outlines a step-by-step path for developing an insider threat program within any organization, focusing on management and employee engagement, as well as ethical, legal, and privacy concerns. In addition, it includes tactics on how to collect, correlate, and visualize potential risk indicators into a seamless system for protecting an organization's critical assets from malicious, complacent, and ignorant insiders. Insider Threat presents robust mitigation strategies that will interrupt the forward motion of a potential insider who intends to do harm to a company or its employees, as well as an understanding of supply chain risk and cyber security, as they relate to insider threat. Offers an ideal resource for executives and managers who want the latest information available on protecting their organization's assets from this growing threat Shows how departments across an entire organization can bring disparate, but related, information together to promote the early identification of insider threats Provides an in-depth explanation of mitigating supply chain risk Outlines progressive approaches to cyber security

Hands-On Cybersecurity for Finance Jan 12 2021 This is a comprehensive guide to help you understand the current threats faced by the financial cyberspace and how to go about it and secure your financial landscape. The book will take you on a journey from identifying the attackers to securing your financial transactions and assets. The book then take you through the updates needed for ...

Insider Threats Aug 31 2022 High-security organizations around the world face devastating threats from insiders—trusted employees with access to sensitive information, facilities, and materials. From Edward Snowden to the Fort Hood shooter to the theft of nuclear materials, the threat from insiders is on the front page and at the top of the policy agenda. Insider Threats offers detailed case studies of insider disasters across a range of different types of institutions, from biological research laboratories, to nuclear power plants, to the U.S. Army. Matthew Bunn and Scott D. Sagan outline cognitive and organizational biases that lead organizations to downplay the insider threat, and they synthesize "worst practices" from these past mistakes, offering lessons that will be valuable for any organization with high security and a lot to lose. Insider threats pose dangers to anyone who handles information that is secret or proprietary, material that is highly valuable or hazardous, people who must be protected, or facilities that might be sabotaged. This is the first book to offer in-depth case studies across a range of industries and contexts, allowing entities such as nuclear facilities and casinos to learn from each other. It also offers an unprecedented analysis of terrorist thinking about using insiders to get fissile material or sabotage nuclear facilities.

Big Data Analytics with Applications in Insider Threat Detection Jul 18 2021 Today's malware mutates randomly to avoid detection, but reactively adaptive malware is more intelligent, learning and adapting to new computer defenses on the fly. Using the same algorithms that antivirus software uses to detect viruses, reactively adaptive malware deploys those algorithms to outwit antivirus defenses and to go undetected. This book provides details of the tools, the types of malware the tools will detect, implementation of the tools in a cloud computing framework and the applications for insider threat detection.

The Insider Threat Jun 16 2021 This book provides emergent knowledge relating to physical, cyber, and human risk mitigation in a practical and readable approach for the corporate environment. It presents and discusses practical applications of risk management techniques along with useable practical policy change options. This practical organizational security management approach examines multiple aspects of security to protect against physical, cyber, and human risk. A practical more tactical focus includes managing vulnerabilities and applying countermeasures. The book guides readers to a greater depth of understanding and action-oriented options.

Managing the Insider Threat Feb 10 2021 Managing the Insider Threat: No Dark Corners and the Rising Tide Menace, Second Edition follows up on the success of – and insight provided by – the first edition, reframing the insider threat by distinguishing between sudden impact and slow onset (aka “rising tide”) insider attacks. This edition is fully updated with coverage from the previous edition having undergone extensive review and revision, including updating citations and publications that have been published in the last decade. Three new chapters drill down into the advanced exploration of rising tide threats, examining the nuanced complexities and presenting new tools such as the loyalty ledger (Chapter 10) and intensity scale (Chapter 11). New explorations of ambiguous situations and options for thwarting hostile insiders touch on examples that call for tolerance, friction, or radical turnaround (Chapter 11). Additionally, a more oblique discussion (Chapter 12) explores alternatives for bolstering organizational resilience in circumstances where internal threats show signs of gaining ascendancy over external ones, hence a need for defenders to promote clearer thinking as a means of enhancing resilience against hostile insiders. Coverage goes on to identify counters to such pitfalls, called lifelines, providing examples of questions rephrased to encourage clear thinking and reasoned debate without inviting emotional speech that derails both. The goal is to redirect hostile insiders, thereby offering alternatives to bolstering organizational resilience – particularly in circumstances where internal threats show signs of gaining ascendancy over external ones, hence a need for defenders to promote clearer thinking as a means of enhancing resilience against hostile insiders. Defenders of institutions and observers of human rascality will find, in Managing the Insider Threat, Second Edition, new tools and applications for the No Dark Corners approach to countering a vexing predicament that seems to be increasing in frequency, scope, and menace.

The Insider Threat Jul 26 2019 In the eighth action-packed thriller in the New York Times bestselling Pike Logan series, ISIS, the most maniacal terrorist organization the modern world has ever seen, is poised to make their most audacious strike yet. The United States has anticipated and averted countless attacks from terrorist groups—thanks in large part to the extralegal counterterrorist unit known as the Taskforce. But now, a much more insidious evil is about to shatter the false sense of safety surrounding civilized nations. While world powers combat ISIS on the battlefield, a different threat is set in motion by the group—one that can’t be defeated by an airstrike. Off the radar of every Western intelligence organization, able to penetrate America or any European state, they intend to commit an act of unimaginable barbarity. Only Pike Logan and the Taskforce stand in the way of an attack no one anticipates, a grand deception that will wreak unthinkable chaos and reverberate throughout the Western world.

Inside Jobs Feb 22 2022 Three cybersecurity veterans reveal how businesses can protect their data from employee error and other internal risks. Written by top leaders at data security company Code42, Inside Jobs offers companies of all sizes a new way to avoid compromising sensitive company data—without slowing business down. Modern-day data security can no longer be accomplished by “Big Brother” forms of monitoring or traditional prevention solutions that rely solely on classification and blocking systems. These technologies frustrate employees, impede collaboration, and force productivity workarounds that risk the very data you need to secure. They provide the illusion that your trade secrets, customer lists, patents, and other intellectual property are protected. That couldn’t be further from the truth, as insider threats continue to grow. These include: Well-intentioned employees inadvertently sharing proprietary data Departing employees taking your trade secrets with them to the competition A high-risk employee moving source code to an unsanctioned cloud service What’s the solution? It’s not the hunt for hooded, malicious wrongdoers that you might expect. The new world of data security is built on security acting as an ally versus an adversary. It assumes positive intent, creates organizational transparency, establishes acceptable data use policies, increases security awareness, and provides ongoing training. Whether you are a CEO, CIO, CISO, CHRO, general counsel, or business leader, this *book will help you understand the important role you have to play in securing the collaborative cultures of the future.*

Insider Threats in Cyber Security Mar 14 2021 Insider Threats in Cyber Security is a cutting edge text presenting IT and non-IT facets of insider threats together. This volume brings together a critical mass of well-established worldwide researchers, and provides a unique multidisciplinary overview. Monica van Huystee, Senior Policy Advisor at MCI, Ontario, Canada comments "The book will be a must read, so of course I'll need a copy." Insider Threats in Cyber Security covers all aspects of insider threats, from motivation to mitigation. It includes how to monitor insider threats (and what to monitor for), how to mitigate insider threats, and related topics and case studies. Insider Threats in Cyber Security is intended for a professional audience composed of the military, government policy makers and banking; financing companies focusing on the Secure Cyberspace industry. This book is also suitable for advanced-level students and researchers in computer science as a secondary text or reference book.

Privileged Attack Vectors Sep 27 2019 See how privileges, passwords, vulnerabilities, and exploits can be combined as an attack vector and breach any organization. Cyber attacks continue to increase in volume and sophistication. It is not a matter of if, but when, your organization will be breached. Attackers target the perimeter network, but, in recent years, have refocused their efforts on the path of least resistance: users and their privileges. In decades past, an entire enterprise might be sufficiently managed through just a handful of credentials. Today's environmental complexity means privileged credentials are needed for a multitude of different account types (from domain admin and sysadmin to workstations with admin rights), operating systems (Windows, Unix, Linux, etc.), directory services, databases, applications, cloud instances, networking hardware, Internet of Things (IoT), social media, and more. When unmanaged, these privileged credentials pose a significant threat from external hackers and insider threats. There is no one silver bullet to provide the protection you need against all vectors and stages of an attack. And while some new and innovative solutions will help protect against or detect the initial infection, they are not guaranteed to stop 100% of malicious activity. The volume and frequency of privilege-based attacks continues to increase and test the limits of existing security controls and solution implementations. Privileged Attack Vectors details the risks associated with poor privilege management, the techniques that hackers and insiders leverage, and the defensive measures that organizations must adopt to protect against a breach, protect against lateral movement, and improve the ability to detect hacker activity or insider threats in order to mitigate the impact. What You'll Learn Know how identities, credentials, passwords, and exploits can be leveraged to escalate privileges during an attack Implement defensive and auditing strategies to mitigate the threats and risk Understand a 12-step privileged access management Implementation plan Consider deployment and scope, including risk, auditing, regulations, and oversight solutions Who This Book Is For Security management professionals, new security professionals, and auditors looking to understand and solve privileged escalation threats

*Enemy at the Water Cooler Dec 23 2021 The book covers a decade of work with some of the largest commercial and government agencies around the world in addressing cyber security related to malicious insiders (trusted employees, contractors, and partners). It explores organized crime, terrorist threats, and hackers. It addresses the steps organizations must take to address insider threats at a people, process, and technology level. Today's headlines are littered with news of identity thieves, organized cyber criminals, corporate espionage, nation-state threats, and terrorists. They represent the next wave of security threats but still possess nowhere near the devastating potential of the most insidious threat: the insider. This is not the bored 16-year-old hacker. We are talking about insiders like you and me, trusted employees with access to information - consultants, contractors, partners, visitors, vendors, and cleaning crews. Anyone in an organization's building or networks that possesses some level of trust. * Full coverage of this hot topic for virtually every global 5000 organization, government agency, and individual interested in security. * Brian Contos is the Chief Security Officer for one of the most well known, profitable and respected security software companies in the U.S.—ArcSight.*

Human-Computer Interaction and Cybersecurity Handbook Dec 31 2019 Recipient of the SJSU San Jose State University Annual Author & Artist Awards 2018 Cybersecurity, or information technology security, focuses on protecting computers and data from criminal behavior. The understanding of human performance, capability, and behavior is one of the main areas that experts in cybersecurity focus on, both from a human–computer interaction point of view, and that of human factors. This handbook is a unique source of information from the human factors perspective that covers all topics related to the discipline. It includes new areas such as smart networking and devices, and will be a source of information for IT specialists, as well as other disciplines such as psychology, behavioral science, software engineering, and security management. Features Covers all areas of human–computer interaction and human factors in cybersecurity Includes information for IT specialists, who often *desire more knowledge about the human side of cybersecurity Provides a reference for other disciplines such as psychology, behavioral science, software engineering, and security management Offers a source of information for cybersecurity practitioners in government agencies and private enterprises Presents new areas such as smart networking and devices*