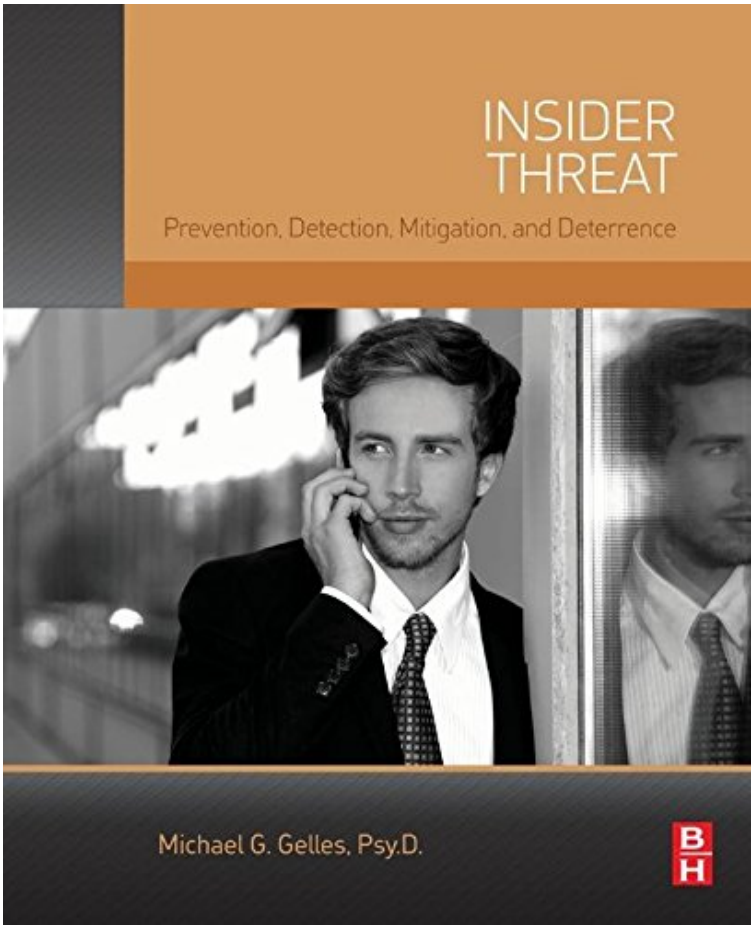
Insider Threat: Prevention, Detection, Mitigation, and Deterrence

Michael G. Gelles
*ePub | *DOC | audiobook | ebooks | Download PDF*



#857214 in eBooks 2016-05-28 2016-05-28File Name: B01GE2S8UQ | File size: 32.Mb

Michael G. Gelles : Insider Threat: Prevention, Detection, Mitigation, and Deterrence before purchasing it in order to gage whether or not it would be worth my time, and all praised Insider Threat: Prevention, Detection, Mitigation, and Deterrence:

4 of 4 people found the following review helpful. Excellent reference in which to use to build your insider threats awareness programBy Ben RothkeInsider threats have been the bane of organizations from time immemorial. When it comes to data threats, for over a decade, the CERT Insider Threat Center has been dedicated to combatting cybersecurity insider threats. Their scientific-based research is the gold standard on the topic.In the newly released Insider Threat: Prevention, Detection, Mitigation, and Deterrence, author Dr. Michael Gelles has added an excellent title to the topic.While the gold standard on the topic is still The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes, this book does add a different angle to the topic, in addition to a lot of timely information and case studies.While the CERT guide is more about the underlying reasons for the insider attacks and crimes, the approach in Gelles is how to build an enterprise program to deal with and defend against insider threats.After providing a few chapters of introduction to the topic and problem, the book details a

systematic method to developing an internal insider threat program.Until I read about it in in the book, I had never heard of the Holistic Management of Employee Risk (HoMER), from the UK-based Centre for the Protection of National Infrastructure. HoMER provides guidance on organizational governance, security culture, and controls to help firms mitigate people risk. Like the CERT Insider Threat Center, HoMER has a significant amount of helpful material.While many consider insiders to be employees, the book does a very good job of showing how to deal with other types of insiders, such as trusted vendors. Gelles reminds the reader of Edward Snowden, whose insider disclosure is perhaps the greatest insider breach today.Aside from mentioning Marigold, a Deloitte software tool, Gelles seems to want to keep the book vendor agnostic and does not list any hardware or software tools that can be used for insider threat detection. Personally, I would have appreciated it had he created a list of such tools, as they are a crucial part of an insider threat program.The book has a significant amount of charts and graphs which are invaluable in communicating to management the crucial importance of an insider threat program.Insider threat exists within every organization, so this book is all reality, no theory. For those looking for a guide in which they can use to start the development of an insider threat detection program, Insider Threat: Prevention, Detection, Mitigation, and Deterrence is a most worthwhile reference.2 of 3 people found the following review helpful. A must for Insider Threat Program Managers.By Jim EastI highly recommend this book for anyone considering developing an Insider Threat program, as well of those of currently managing Insider Threat programs. Very well written, and laid out in a manner that makes a good reference book.

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 organizationrsquo;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 organizationrsquo;s assets from this growing threatShows how departments across an entire organization can bring disparate, but related, information together to promote the early identification of insider threatsProvides an in-depth explanation of mitigating supply chain riskOutlines progressive approaches to cyber security

"...well structured and well written. The visuals throughout the book and key takeaways at the end of each chapter are practical and insightfulhellip;of great value to the professional who manages or aspires to manage the prevention, detection, response, and deterrence of insider threats." --Security ManagementAbout the AuthorDr. Michael Gelles consults in security, intelligence, and law enforcement for Deloitte in Washington, D.C. and is a thought-leader on the security risks, asset exploitation, and workplace violence associated with insider threat. Dr. Gelles is a frequent lecturer and has written numerous articles and book chapters on organizational management, forensic psychology, law enforcement, terrorism, and counterintelligence.