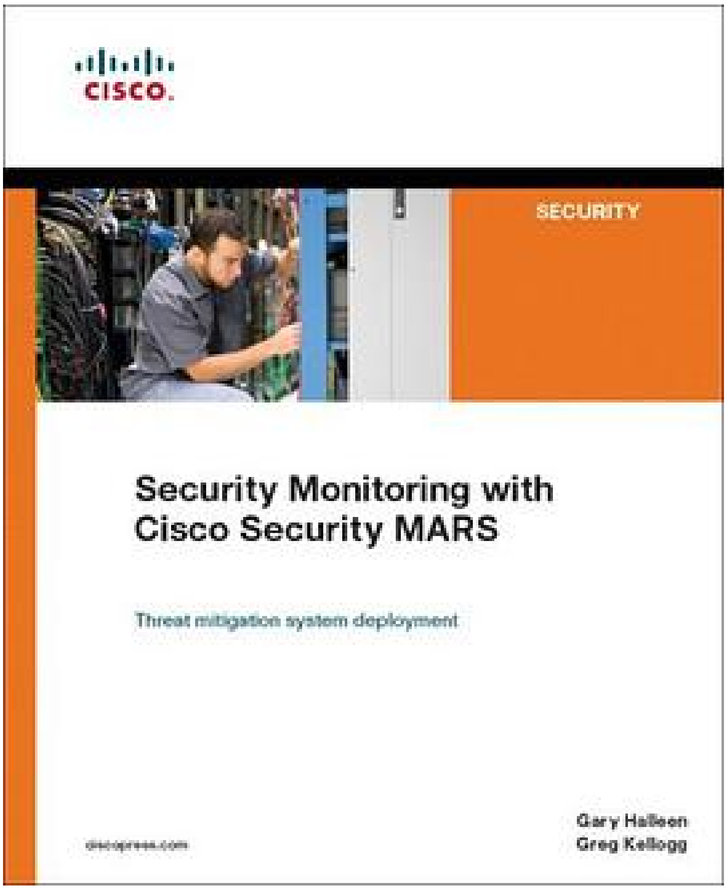
Security Monitoring with Cisco Security MARS (Networking Technology


cisco.
SECURITY
Security Monitoring with Cisco Security MARS
Threat mitigation system deployment
ciscopress.com
Gary Halleen
Greg Kellogg

Security Monitoring with Cisco Security MARS (Networking Technology_下载链接1_

著者:Gary Halleen

出版者:Cisco Press

出版时间:2007-07-16

装帧:Paperback

isbn:9781587052705

Security Monitoring with Cisco Security MARS Threat mitigation system deployment Gary Halleen Greg Kellogg Networks and hosts are probed hundreds or thousands of times a day in an attempt to discover vulnerabilities. An even greater number of automated attacks from worms and viruses stress the same devices. The sheer volume of log messages or events generated by these attacks and probes, combined with the complexity of an analyst needing to use multiple monitoring tools, often makes it impossible to adequately investigate what is happening. Cisco(R) Security Monitoring, Analysis, and Response System (MARS) is a next-generation Security Threat Mitigation system (STM). Cisco Security MARS receives raw network and security data and performs correlation and investigation of host and network information to provide you with actionable intelligence. This easy-to-use family of threat mitigation appliances enables you to centralize, detect, mitigate, and report on priority threats by leveraging the network and security devices already deployed in a network, even if the devices are from multiple vendors. Security Monitoring with Cisco Security MARS helps you plan a MARS deployment and learn the installation and administration tasks you can expect to face. Additionally, this book teaches you how to use the advanced features of the product, such as the custom parser, Network Admission Control (NAC), and global controller operations. Through the use of real-world deployment examples, this book leads you through all the steps necessary for proper design and sizing, installation and troubleshooting, forensic analysis of security events, report creation and archiving, and integration of the appliance with Cisco and third-party vulnerability assessment tools. "In many modern enterprise networks, Security Information Management tools are crucial in helping to manage, analyze, and correlate a mountain of event data. Greg Kellogg and Gary Halleen have distilled an immense amount of extremely valuable knowledge in these pages. By relying on the wisdom of Kellogg and Halleen embedded in this book, you will vastly improve your MARS deployment." -Ed Skoudis, Vice President of Security Strategy, Predictive Systems Gary Halleen is a security consulting systems engineer with Cisco. He has in-depth knowledge of security systems as well as remote-access and routing/switching technology. Gary is a CISSP and ISSAP. His diligence was responsible for the first successful computer crimes conviction in the state of Oregon. Gary is a regular speaker at security events and presents at Cisco Networkers conferences. Greg Kellogg is the vice president of security solutions for Calence, LLC. He is responsible for managing the company's overall security strategy. Greg has more than 15 years of networking industry experience, including serving as a senior security business consultant for the Cisco Enterprise Channel organization. Additionally, Greg worked for Protego Networks, Inc. (where MARS was originally developed). There he was responsible for developing channel partner programs and helped solution providers increase their security revenue. Learn the differences between various log aggregation and correlation systems * Examine regulatory and industry requirements * Evaluate various deployment scenarios * Properly size your deployment * Protect the Cisco Security MARS appliance from attack * Generate reports, archive data, and implement disaster recovery plans * Investigate incidents when Cisco Security MARS detects an attack * Troubleshoot Cisco Security MARS operation * Integrate Cisco Security MARS with Cisco Security Manager, NAC, and third-party devices * Manage groups of MARS controllers with global controller operations This security book is part of the Cisco Press(R) Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end self-defending networks. Category: Cisco Press-Security Covers: Security Threat Mitigation

作者介绍:

目录:

Security Monitoring with Cisco Security MARS (Networking Technology_下载链接1_

标签

评论

Security Monitoring with Cisco Security MARS (Networking Technology_下载链接1_

书评

Security Monitoring with Cisco Security MARS (Networking Technology_下载链接1_