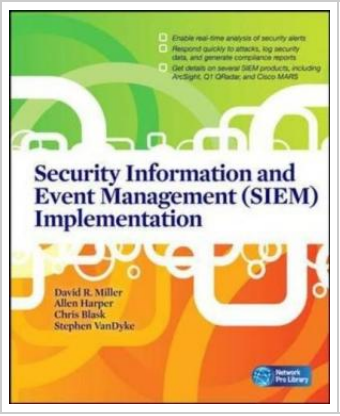

Security Information and Event Management (SIEM) Implementation (Paperback)

By David R. Miller, Allen Harper, Zachary Payton

McGraw-Hill Education - Europe, United States, 2010. Paperback. Condition: New. Language: English . Brand New Book. Implement a robust SIEM system Effectively manage the security information and events produced by your network with help from this authoritative guide. Written by IT security experts, Security Information and Event Management (SIEM) Implementation shows you how to deploy SIEM technologies to monitor, identify, document, and respond to security threats and reduce false-positive alerts. The book explains how to implement SIEM products from different vendors, and discusses the strengths, weaknesses, and advanced tuning of these systems. You ll also learn how to use SIEM capabilities for business intelligence. Real-world case studies are included in this comprehensive resource. Assess your organization s business models, threat models, and regulatory compliance requirements Determine the necessary SIEM components for small- and medium-size businesses Understand SIEM anatomy-source device, log collection, parsing/normalization of logs, rule engine, log storage, and event monitoring Develop an effective incident response program Use the inherent capabilities of your SIEM system for business intelligence Develop filters and correlated event rules to reduce false-positive alerts Implement AlienVault s Open Source Security Information Management (OSSIM) Deploy the Cisco Monitoring Analysis and Response System (MARS) Configure and use the...

Reviews

This created ebook is great. it was writtern very properly and useful. Its been printed in an exceedingly easy way in fact it is just right after i finished reading this pdf where basically modified me, alter the way i think.

-- ***Aglae Becker***

This ebook is definitely worth buying. It is definitely basic but excitement within the fifty percent in the ebook. Its been designed in an extremely straightforward way which is merely following i finished reading this ebook where basically changed me, alter the way in my opinion.

-- ***Ward Morar***