

Applied network security monitoring : collection, detection, and analysis

Sanders, Chris, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20426799&lokasi=lokal>

Abstrak

Applied network security monitoring is the essential guide to becoming an NSM analyst from the ground up. This book takes a fundamental approach to NSM, complete with dozens of real-world examples that teach you the key concepts of NSM.

Network security monitoring is based on the principle that prevention eventually fails. In the current threat landscape, no matter how much you try, motivated attackers will eventually find their way into your network. At that point, it is your ability to detect and respond to that intrusion that can be the difference between a small incident and a major disaster.

The book follows the three stages of the NSM cycle: collection, detection, and analysis. As you progress through each section, you will have access to insights from seasoned NSM professionals while being introduced to relevant, practical scenarios complete with sample data.