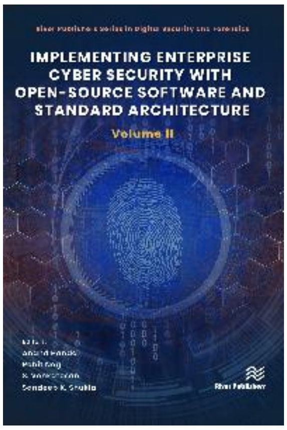
River Publishers



River Publishers Series in Digital Security and Forensics

IMPLEMENTING ENTERPRISE CYBER SECURITY WITH OPEN-SOURCE SOFTWARE AND STANDARD ARCHITECTURE

Volume II

Editors
Anand Handa
Rohit Negi
S. Venkatesan
Sandeep K. Shukla

River Publishers

River Publishers Series in Digital Security and Forensics

Implementing Enterprise Cyber Security with Open-Source Software and Standard Architecture: Volume II

Editors:
Anand Handa, C3i Center, Indian Institute of Technology, Kanpur, India
Rohit Negi, C3i Center, Indian Institute of Technology, Kanpur, India
S. Venkatesan, Indian Institute of Information Technology Allahabad, India
Sandeep K. Shukla, C3i Center, Indian Institute of Technology, Kanpur, India

ISBN: 9788770227957
e-ISBN: 9788770227940
Available From: October 2022
Price: € 104.50

Description:

Cyber security is one of the most critical problems faced by enterprises, government organizations, education institutes, small and medium scale businesses, and medical institutions today. Creating a cyber security posture through proper cyber security architecture, deployment of cyber defense tools, and building a security operation center are critical for all such organizations given the preponderance of cyber threats. However, cyber defense tools are expensive, and many small and medium-scale business houses cannot procure these tools within their budgets. Even those business houses that manage to procure them cannot use them effectively because of the lack of human resources and the knowledge of the standard enterprise security architecture. In 2020, the C3i Center at the Indian Institute of Technology Kanpur developed a professional certification course where IT professionals from various organizations go through rigorous six-month long training in cyber defense. During their training, groups within the cohort collaborate on team projects to develop cybersecurity solutions for problems such as malware analysis, threat intelligence collection, endpoint detection and protection, network intrusion detection, developing security incidents, event management systems, etc. All these projects leverage open-source tools, and code from various sources, and hence can be also constructed by others if the recipe to construct such tools is known. It is therefore beneficial if we put these recipes out in the form of book chapters such that small and medium scale businesses can create these tools based on open-source components, easily following the content of the chapters. In 2021, we published the first volume of this series based on the projects done by cohort 1 of the course. This volume, second in the series has new recipes and tool development expertise based on the projects done by cohort 3 of this training program. This volume consists of nine chapters that describe experience and know-how of projects in malware analysis, web application security, intrusion detection system, and honeypot in sufficient detail so they can be recreated by anyone looking to develop home grown solutions to defend themselves from cyber-attacks.

Keywords: Honeypot, Honeynet, Open-Source Security Tools, Web Security, Application Security, Database Security, Network Security, Threat Intelligence, Threat Analytics, Network Analytics, Malware Analysis, Cuckoo Sandbox, Machine Learning, Static and Dynamic Analysis, NIDS, HIDS, SOC, Security Architecture, SIEM, Firewall, Virtualization, Phishing Detection, Android Application, Feature Engineering

Denmark Head Office
Alsbjergvej 10
9260 Gistrup
Denmark
www.riverpublishers.com
Email: info@riverpublishers.com

USA Office
Indianapolis, IN
USA
Tel.: +1-3176899634
Email: rajeev.prasad@riverpublishers.com

UK Office
River Publishers
Email: philippa.jefferies@riverpublishers.com