Proceedings

WOSOC 2023

Workshop on
Security Operation Center
Operations and Construction

February 27, 2023
San Diego, CA, USA

Published by the

Internet
Society

Internet Society
11710 Plaza America Drive
Suite 400
Reston, VA 20190

This volume is published as a collective work. The Internet Society owns the copyright for this publication and the copyrights to the individual papers are retained by their respective author[s].

Address your correspondence to: NDSS Program Manager, Internet Society, 11710 Plaza America Drive, Suite 400, Reston, VA 20190 USA, tel. +1 703 439 2120, fax +1 703 326 9881, ndss@elists.isoc.org.

The papers included here comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interest of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors or the Internet Society.

ISBN Number (Digital Format) 1-891562-90-8

Additional copies may be ordered from:

Internet Society
11710 Plaza America Drive
Suite 400
Reston, VA 20190
tel +1 703.439.2120
fax +1 703.326.9881
http://www.internetsociety.org

Proceedings of WOSOC 2023 – Workshop on Security Operation Center Operations and Construction

Table of Contents

Message from the Program Co-Chairs

Welcome to the first Workshop on Security Operations Center Operations and Construction (WOSOC), held February 27, 2023, on the first day of the Network and Distributed Systems Security (NDSS) Symposium in San Diego, California.

WOSOC was created to address the growing recognition across academic and operations security communities that Security Operation Center (SOC) operations were an important topic for study and systematic analysis. In the last 20 years, SOCs have become an increasingly central to security operation. SOC operators are recognized as a distinct class of security professionals who need tools and practices that address the distinct challenges and insights of their discipline. In parallel to this increased professionalization by the operational community is an increased interest in the academic community: researchers are studying SOC processes, workflows, and training.

The WOSOC workshop is designed to enable researchers and operators to meet, see each other's work, and exchange ideas about how to improve the state of the practice in security operations. This year has representatives from both communities present and an even split in presentations from both communities.

We hope to see more submissions in the future and for more exchanges to happen. Here's to seeing you in 2024.

Michael Collins and Nolen Scaife
Program Committee Co-Chairs, WOSOC 2023

Program Committee Co-Chairs

Michael Collins, *USC Information Sciences Institute*
Nolen Scaife, *Walmart*

Program Committee

Alefiya Hussain, *USC Information Sciences Institute*
Stephen Schwab, *USC Information Sciences Institute*
Dan Massey, *USC Information Sciences Institute*
Wes Hardaker, *USC Information Sciences Institute*
Ganesh Sankaran, *USC Information Sciences Institute*
David Balenson, *USC Information Sciences Institute*
Xinming Ou, *University of South Florida*
Scott Tousley, *IT Cadre*
Scott Rose, *National Institute of Standards and Technology*
Kevin Butler, *University of Florida*
Josiah Dykstra, *National Security Agency*