enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

HOW TO SETUP UP CSIRT AND SOC

GOOD PRACTICE GUIDE

DECEMBER 2020

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For queries in relation to this study, please use: csirt-relations@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Edgars Taurins, ENISA.
Activities supporting this study were conducted under contract with NRD Cyber Security.

ACKNOWLEDGEMENTS

Study was performed with the input from Informal Expert Group on EU Member States Incident Response Development.

LEGAL NOTICE

Copyright notice

ISBN 978-92-9204-410-7 - DOI 10.2824/056764

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This publication provides results-driven guidance for those who are interested in establishing a computer security incident response team (CSIRT) or security operations centre (SOC), and guidance on possible improvements for different types of CSIRTs and SOCs that exist currently.

The content of this report is based on an analysis of current publications on the establishment of CSIRTs (the analysis is summarised in Annex B); a field questionnaire (Annex A), which was completed by 40 CSIRTs and SOCs; and the authors' experiences in establishing and improving CSIRTs as part of numerous projects carried out in Europe, Asia, Africa and South America.

A results-driven approach is taken throughout the publication to provide guidance on the different stages involved in the establishment of a CSIRT or SOC organisation:

- Assessment for readiness
- Design
- Implementation
- Operations
- Improvement.

The reader will receive practical guidance on what to focus on during the individual phases of establishment and improvement.

Up to July 2020, ENISA had published 61 reports and 21 translated versions of reports supporting CSIRTs on its website ([1]). ENISA's training package ([2]) provides online training materials, training courses and exercise materials for cybersecurity specialists, based on the 'Train the Trainer' philosophy. This document aims to enhance ENISA's existing body of knowledge on the establishment of CSIRTs.

[1] https://www.enisa.europa.eu/publications#c8=CSIRTs
[2] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/