GFCE GLOBAL FORUM ON CYBER EXPERTISE

CYBER INCIDENT MANAGEMENT (CIM)

CYBIL PORTAL RESOURCES GUIDE

Last Updated: October 2022

Summary

The Cyber Incident Management (CIM) Cybil Portal Resources Guide is an initiative of the GFCE Working Group B CIM Task Force.

Context

During the June 2022 in-person GFCE CIM TF Meeting in the margins of the 34th Annual FIRST Conference, members of the CIM TF examined and discussed the Cybil Portal resources (Tools and Publications) that were under the topic of the Task Force (Cyber Incident Management) on the Cybil Knowledge Portal.

After careful consideration and revision of all these resources, the Task Force decided to continue this discussion by adding those who they found relevant and were missing to the Cybil Portal and ultimately creating a useful and simple guide for the Task Force and the CIM Community in general.

Aim

The objective of this guide is to provide an overview of all the resources that are available for the CIM community on the Cybil Portal as of October 2022. By doing this, we hope that users of the Cybil Portal will be able to navigate through all the cyber incident management resources available in an easier and more focused manner. In addition, this guide intends to help users build their cyber capacity according to their various different needs. For this reason, the resources are classified into different practical sections so that users can adapt them to their different needs. This way, if users want to, for instance, find out tools and resources that will help them build a CSIRT or want to measure their organisational incident management maturity, they can freely make use of the most relevant resources available in the field.

Cybil Cyber Incident Management Resources – Table of Contents

CSIRT Establishment Guides

Title	Year	Source	Publication type	URL
Getting started with a National CSIRT guide	2021	TNO	Guide	https://cybilportal.org/publications/getting-started-with-a-national-csirt-guide/
The Sector CSIRT Framework: Developing Sector-Based Incident Response Capabilities	2021	CMU SEI	Guide	https://cybilportal.org/publications/the-sector-csirt-framework-developing-sector-based-incident-response-capabilities/
ITU cybersecurity programme: CIRT framework	2021	ITU	Guide	https://cybilportal.org/publications/building-a-soc-start-small/
How to set up CSIRT and SOC: Good practice Guide	2020	ENISA; NRD Cyber Security	Guide	https://cybilportal.org/publications/how-to-set-up-csirt-and-soc-good-practice-guide/
GFCE Global Good Practices – National Computer Incident Response Teams (CSIRTs)	2017	GFCE	Report; Study	https://cybilportal.org/publications/global-good-practices-national-computer-security-incident-response-teams-csirts/
Establishing a CSIRT	2017	ThaiCERT	Guide	https://cybilportal.org/publications/establishing-a-csirt/
Building a SOC: start small	2017	National Cyber Security Centre, The Netherlands	Guide	https://cybilportal.org/publications/building-a-soc-start-small/
Best Practices for Establishing a National CSIRT	2016	OAS	Guide	https://cybilportal.org/publications/best-practices-for-establishing-a-national-csirt-by-the-organisation-of-american-states-oas/
Create a CSIRT	2017	CMU SEI	Guide	https://cybilportal.org/publications/sei-create-a-csirt/

Developing of CSIRT

Title	Year	Source	Publication type	URL
Cyber Incident Management in Low-Income Countries	2022	GFCE; Global Affairs Canada (Affaires Mondiales Canada); AfricaCERT	Report	https://cybilportal.org/publications/cyber-incident-management-in-low-income-countries-part-1-a-holistic-view-on-csirt-development/
11 Strategies of A World-Class Cybersecurity Operations Center	2022	MITRE	Report	https://cybilportal.org/publications/61561/
Computer Security Incident Response Team (CSIRT) Services Framework	2019	FIRST.org	Report	https://cybilportal.org/publications/first-csirt-services-framework-version-2-1/
CSIRT Training Materials of ENISA	2019	ENISA	Guide	https://cybilportal.org/publications/enisa-csirt-maturity-framework/

Measuring Maturity

Title	Year	Source	Publication type	URL
ENISA CSIRT Maturity Framework - Updated and improved	2022	ENISA	Report	https://cybilportal.org/publications/enisa-csirt-maturity-framework/
SIM3 assessment tool	2022	Open CSIRT Foundation	Tool	https://cybilportal.org/publications/sim3-self-assessment-tool/
SOC-CMM and SOC-CMM 4CERT	2022	SOC-CMM	Tool	https://cybilportal.org/publications/soc-cmm/
The Global CSIRT Maturity Framework	2021	GFCE	Tool	https://cybilportal.org/publications/global-csirt-maturity-framework/
SIM3: Security Incident Management Maturity Model	2015	Open CSIRT Foundation	Report	https://cybilportal.org/publications/sim3-security-incident-management-maturity-mod
CSIRT Maturity Kit	2015	National Cyber Security Centre, The Netherlands	Report	https://cybilportal.org/publications/csirt-maturity-kit/

Information Sharing and Management

Title	Year	Source	Publication type	URL
Cyber Threat Intelligence Sharing	2021	UK FCDO; Citi Bank	Report	https://cybilportal.org/publications/cyber-threat-intelligence-sharing/
Common Taxonomy for Law Enforcement and The National Network of CSIRTs	2017	Europol	Report	https://cybilportal.org/publications/common-taxonomy-for-law-enforcement-and-the-national-network-of-csirts/
Produce and Present Trusted Metrics about Systemic Risk Conditions	2017	GFCE	Tool	https://cybilportal.org/publications/produce-and-present-trusted-metrics-about-systemic-risk-conditions-2/
Establish a Clearinghouse for Gathering Systemic Risk Conditions Data in Global Networks	2017	GFCE	Tool	https://cybilportal.org/publications/establish-a-clearinghouse-for-gathering-systemic-risk-conditions-data-in-global-networks-2/

Incident Response Guides

Title	Year	Source	Publication type	URL
Software Supply Chain Attacks	2021	DHS/CISA; NIST	Report	https://cybilportal.org/publications/software-supply-chain-attacks-cisa-nist/
Ransomware	2021	DHS/CISA; MS-ISAC	Article	https://cybilportal.org/publications/ransomware-cisa/
Joint Cybersecurity Advisory – Technical Approaches to Uncovering and Remediating Malicious Activity	2020	DHS/CISA; UK NCSC; CERT NZ; NCSC NZ; CCCS; ACSC	Tool	https://cybilportal.org/publications/joint-cybersecurity-advisory-technical-approaches-to-uncovering-and-remediating-malicious-activity/

General Information

Title	Year	Source	Publication type	URL
nCSIRT Guide – Self Help	2021	UK FCDO; CSA; Torchlight Group; PGI	Tool	https://cybilportal.org/publications/ncsirt-guide-self-help/
CISA Cybersecurity Resources	2021	DHS/CISA	Article	https://cybilportal.org/publications/cisa-cybersecurity-resources-cisa/

Strategy and Policy

Title	Year	Source	Publication type	URL
Cyber Strategy Development & Implementation (CSDI) Framework	2020	The MITRE Corporation	Tool	https://cybilportal.org/publications/national-cyber-strategy-development-implementation-framework/

CCB Good Practice and Case Studies

Title	Year	Source	Publication type	URL
Western Balkan CERT Cooperation	2021	Open CSIRT Foundation	Report	https://cybilportal.org/publications/western-balkan-cert-cooperation/
DCAF's CSIRT Capacity Building Methodology: Lessons Learned from the Western Balkans	2021	DCAF	Report	https://cybilportal.org/publications/dcafs-csirt-capacity-building-methodology-lessons-learned-from-the-western-balkans/
Cybersecurity – DCAF's Work on CERT Development	2019	DCAF	Report	https://cybilportal.org/publications/cybersecurity-dcafs-work-on-cert-development/

Global Cyber Expertise Magazine

Title	Year	Source	Publication type	URL
Issue 11 – September 2022	2022	GFCE	Article	https://cybilportal.org/publications/global-cyber-expertise-magazine-issue-11-september-2022/
Issue 10 – November 2021	2021	GFCE	Article	https://cybilportal.org/publications/global-cyber-expertise-magazine-issue-10-november-2021/
Issue 9 – June 2021	2021	GFCE	Article	https://cybilportal.org/publications/global-cyber-expertise-magazine-issue-9-june-2021/
Issue 8 – November 2020	2020	GFCE	Article	https://cybilportal.org/publications/global-cyber-expertise-magazine-issue-8-november-2020/
Issue 7 – April 2020	2020	GFCE	Article	https://cybilportal.org/publications/global-cyber-expertise-magazine-issue-7-april-2020/
Issue 6 – October 2019	2019	GFCE	Article	https://cybilportal.org/publications/global-cyber-expertise-magazine-issue-6-october-2019/
Issue 5 – September 2018	2018	GFCE	Article	https://cybilportal.org/publications/global-cyber-expertise-magazine-issue-5-september-2018/
Issue 4 – November 2017	2017	GFCE	Article	https://cybilportal.org/publications/global-cyber-expertise-magazine-issue-4-november-2017/
Issue 3 – May 2017	2017	GFCE	Article	https://cybilportal.org/publications/global-cyber-expertise-magazine-issue-3-may-2017/
Issue 2 – November 2016	2016	GFCE	Article	https://cybilportal.org/publications/global-cyber-expertise-magazine-issue-2-november-2016/
Issue 1 – June 2016	2016	GFCE	Article	https://cybilportal.org/publications/global-cyber-expertise-magazine-issue-1-june-2016/

ITU Global Cybersecurity Index

Title	Year	Source	Publication type	URL
Global Cybersecurity Index (GCI) v4	2019	ITU	Report	https://cybilportal.org/publications/itu-global-cybersecurity-index-gci-v4/
Global Cybersecurity Index (GCI) v3	2017	ITU	Report	https://cybilportal.org/publications/itu-global-cybersecurity-index-gci-v3/
Global Cybersecurity Index (GCI) v2	2015	ITU	Report	https://cybilportal.org/publications/itu-global-cybersecurity-index-gci-v2/
Global Cybersecurity Index (GCI) v1	2013	ITU	Report	https://cybilportal.org/publications/itu-global-cybersecurity-index-gci-v1/