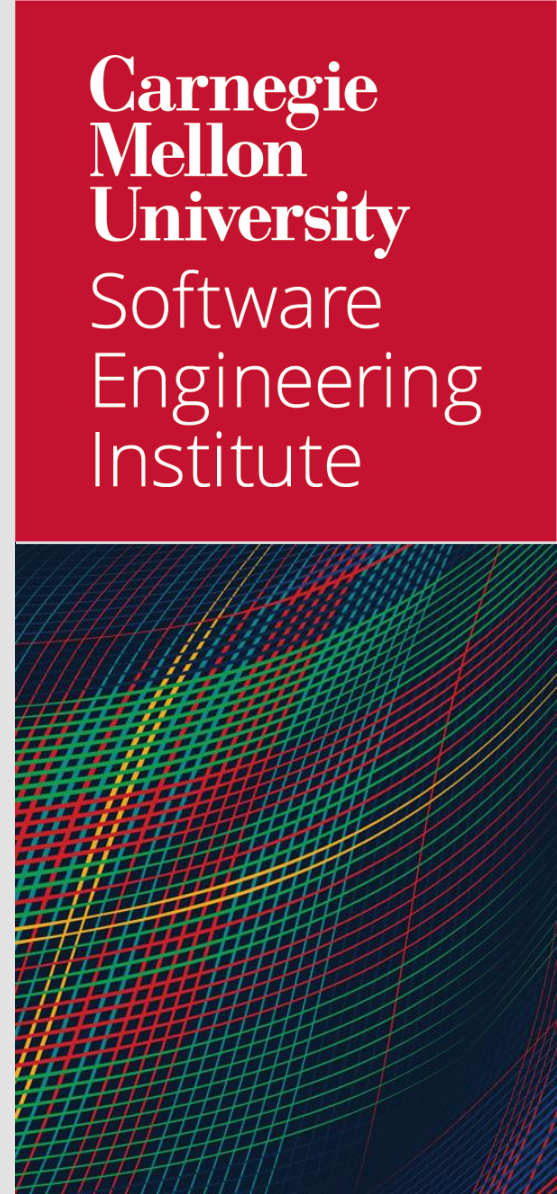


Module 1: Introduction to Planning and Implementing a National/Government CSIRT

Planning and Implementing a National/Government CSIRT



Copyright 2024 Carnegie Mellon University.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

CERT®, Carnegie Mellon® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM24-0005

Introduction

Purpose

To help you

- understand the functions of National or Government Computer Security Incident Response Teams (CSIRTs) and the philosophy behind them
- appreciate the possible roles played by such CSIRTs
- identify some of the challenges faced by these types of CSIRTs
- appreciate the key issues and decisions that must be addressed when creating or operating a National or Government CSIRT

Course Goals



Discuss the unique role of a National or Government CSIRT.

Review the components of a CSIRT in general.

Identify enablers and supporting resources for establishing a National or Government CSIRT.

Characterize Stakeholders for National and Government CSIRTs.

Identify needed collaboration, coordination, and information sharing initiatives and activities.

Discuss planning decisions and strategies.

Identify implementation strategies.

Review methods for evaluating National and Government CSIRTs and implementing resulting process improvements.

Intended Audience




Individuals tasked with creating a National or Government CSIRT or incident management capability

Other individuals who need or would like an understanding of general CSIRT and specifically National CSIRT issues and processes

Individuals interested in learning more about CSIRTs, National CSIRTs, and incident management activities in general

Agenda -1



Module 1: Introduction to Planning and Implementing a National/Government CSIRT

Module 2: National Incident Management Ecosystem

Module 3: Defining Incident Management (IM)

Module 4: The Evolving Nature of Incident Management Capabilities

Module 5: Defining CSIRTs

Module 6: Uniqueness of a National or Government CSIRT

Module 7: National CSIRT Principles

Module 8: Connection with Critical Infrastructures


Module 9: Planning a National or Government CSIRT: Building Your Strategy

Module 10: Planning a National or Government CSIRT: Best Practices

Module 11: Planning a National or Government CSIRT: Key Decisions

Module 12: Implementing Your National or Government CSIRT

Agenda -2

- 
- Module 13: Implementing Your National or Government CSIRT: Roles and Responsibilities
 - Module 14: Implementing Your National or Government CSIRT: Incident Criteria and Incidents of National Importance
 - Module 15: Implementing Your National or Government CSIRT: Incident Reporting Requirements
 - Module 16: Implementing Your National or Government CSIRT: Policies and Procedures
 - Module 17: Implementing Your National or Government CSIRT: Challenges
 - Module 18: Implementing Your National or Government CSIRT: Politics and Policies
 - Module 19: Implementing Your National or Government CSIRT: Branding
 - Module 20: Implementing Your National or Government CSIRT: Information Sharing
 - Module 21: Process Improvement and Sustainment
 - Module 22: Summary
 - Module 23: Resources

Applying Course Materials



Each organization is different.

Refer to your own country, economy, or government rules, regulations, laws, and policies.

Refer and align with your parent organization incident management policies, procedures, and processes for

- established roles and responsibilities
- approved workflows
- appropriate responses and response times
- prioritization and escalation criteria

No Single Recipe

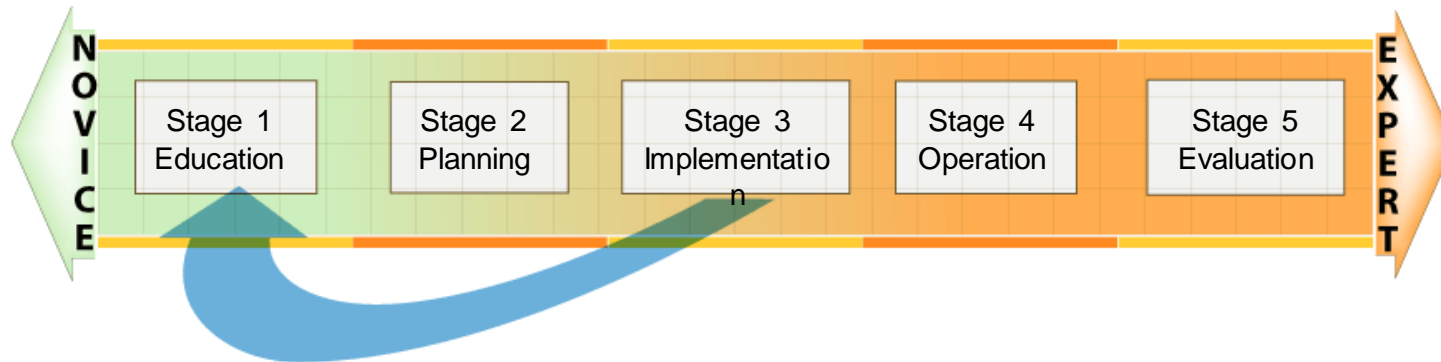
There is no single recipe for creating a CSIRT.

It depends on your

- needs and requirements
- mission and goals
- available resources and support

Stages of CSIRT Development

- Stage 1 Educating the organization
- Stage 2 Planning effort
- Stage 3 Initial implementation
- Stage 4 Operational phase
- Stage 5 Evaluation and improvement



CSIRT Development Continuum

Nascent

An individual or group learning about concepts and operations at the foundational level

Developing

The ability to both plan for and stand up/implement the CSIRT

Capable

The ability to provide and/or operate a CSIRT at an initial operating capacity

Sustaining

The ability to provide and/or operate a CSIRT at a full operating capability that maintains its viability by using continuous process improvement techniques

Contributing Partner

Ability to act as a leader and expert in the community and contribute to the overall growth and improvement of the community.

Leading Edge

The ability to be at the forefront of CSIRT research and development

Some Definitions

Term	Definition
CSIRT	<ul style="list-style-type: none"> • Computer Security Incident Response Team or capability • an organization or capability that provides services and support, to a defined constituency, for preventing, handling, and responding to computer security incidents
National CSIRT	<ul style="list-style-type: none"> • CSIRT with National responsibility • designated to have specific responsibilities in cybersecurity protection for a country or economy
Government CSIRT	<ul style="list-style-type: none"> • can be a CSIRT responsible for cybersecurity strategies and protection for government ministries or departments or a national CSIRT or perform the role of both
Constituency	<ul style="list-style-type: none"> • organization or individuals being served by the CSIRT
Stakeholder	<ul style="list-style-type: none"> • internal or external organizations or individuals who are interested in, support, or partner with the CSIRT

Questions and Discussion

