



# Security Operations Overview

Monitoring and Response Directorate  
CERT Division

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

# Notices

Copyright 2018 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

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.

GOVERNMENT PURPOSE RIGHTS – Technical Data

Contract No.: FA8702-15-D-0002

Contractor Name: Carnegie Mellon University

Contractor Address: 4500 Fifth Avenue, Pittsburgh, PA 15213

The Government's rights to use, modify, reproduce, release, perform, display, or disclose these technical data are restricted by paragraph (b)(2) of the Rights in Technical Data—Noncommercial Items clause contained in the above identified contract. Any reproduction of technical data or portions thereof marked with this legend must also reproduce the markings.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

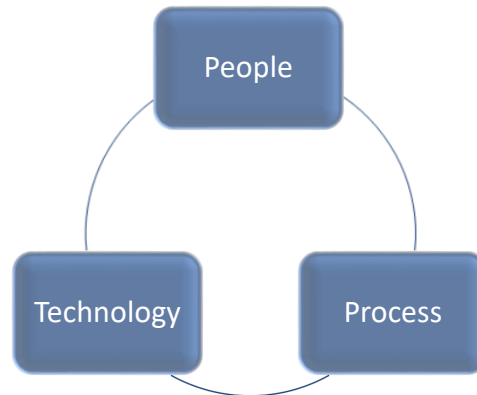
Carnegie Mellon®, CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM18-1314

# Capacity Development: A Multi-Faceted Approach

# Defining the Incident Management Function

An *incident management function* is a set of capabilities (the people, processes, technology, etc. that provide an ability or capacity to perform some task) considered essential to protecting, detecting, and responding to incidents, as well as sustaining the incident management function.

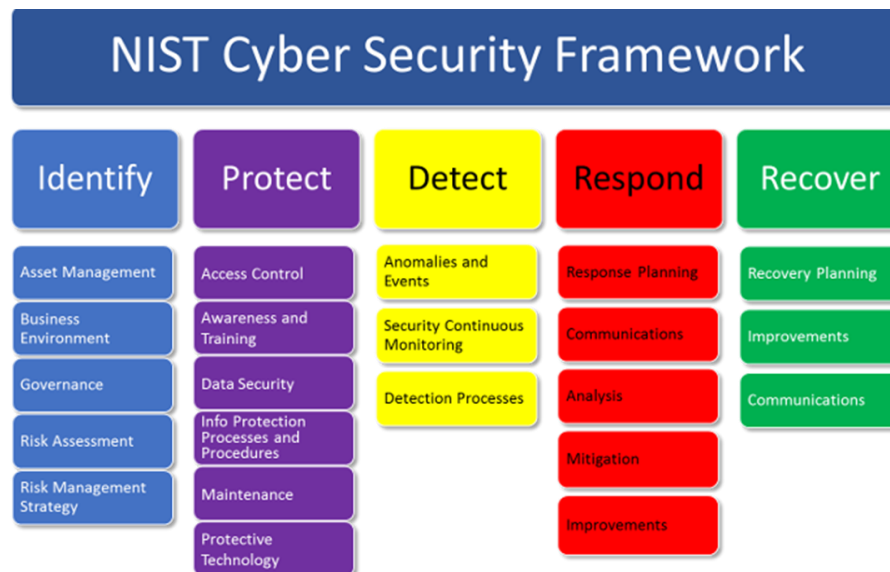


Incident management capabilities can be institutionalized in various entities: CSIRT, SOC, combination, or other organizational structure.

# Organizations Require a Cybersecurity Strategy

Such a strategy should support and enable the organizational mission and corresponding business processes.

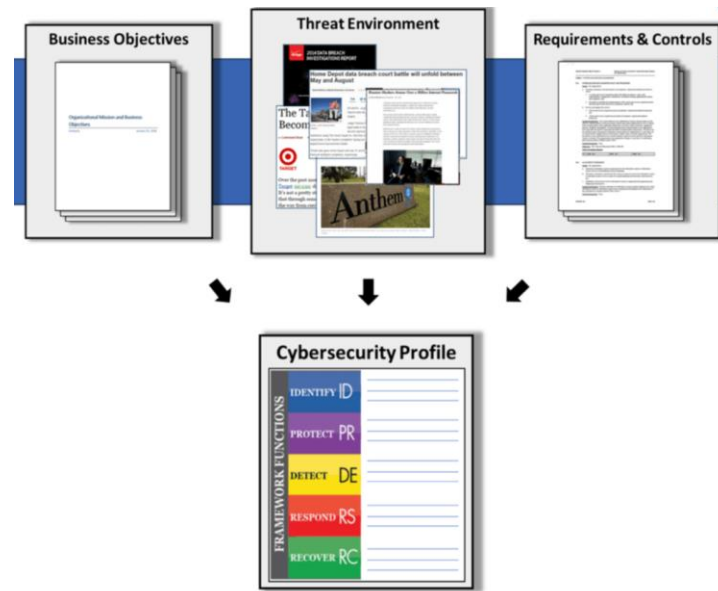
One example of the components involved in such a strategy can be seen in the NIST Cybersecurity Framework.



Source: Introduction to the NIST CyberSecurity Framework for a Landscape of Cyber Menaces. Security Affairs, April 2017. Available at: <http://securityaffairs.co/wordpress/58163/laws-and-regulations/nist-cybersecurity-framework-2.html>

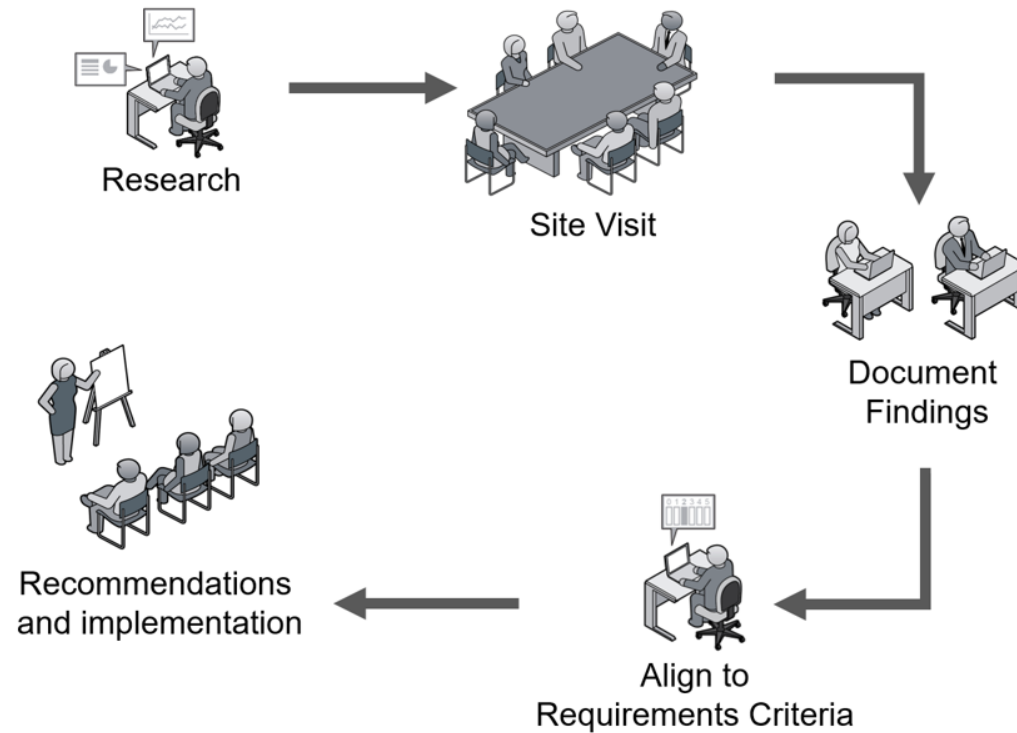
# Framework Profile

- Alignment of the core with the requirements of an organization
- Current vs. Target
- Can be used to develop:
  - Gap analysis
  - Self-assessments
  - Roadmaps

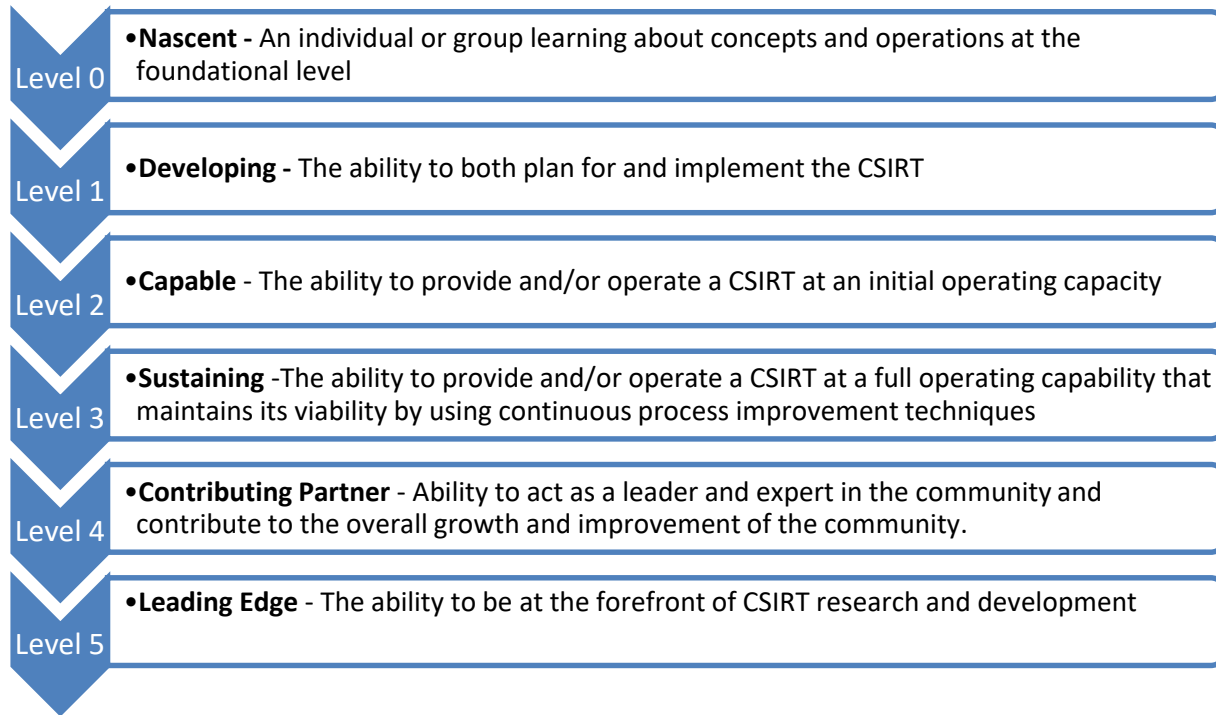


<https://www.nist.gov/cyberframework/online-learning/components-framework>


# CERT Method of Implementation



# Categorization – The CSIRT Capacity Development Continuum







# Security Operations International Cybersecurity Initiatives

# Security Operations Portfolio

## Training and Mentoring

- Public Courses
- On site courses
- Mentoring modules
- On site mentoring
- Train the Trainer
- License training materials
- Computer Security Incident Handling (CSIH) Certification
- Facilitated workshops
- Professional Development
- Competency Development

## Building Capacity

- Building:
  - Capability Metrics for Service Improvement
  - Training and Mentoring Programs
  - Security Operation Centers (collaborative with Solutions Team)
  - Computer Security Incident Response Teams (CSIRTs)
- CSIRT Toolkit
- CSIRT Development Continuum

## Assessment & Evaluation Metrics

- Incident Management Capability Assessment (IMCA)
- Incident Management Mission Risk Diagnostics for Incident Management Capabilities (MRD-IMC)
- National CSIRT Capability Assessment
- SOC Evaluation (Solutions)
- Metrics: SOC, CSIRT, Metrics SIG, Literature search publication

## Developing State of the Art

- Data Analytics/ Machine Learning
- Incident Handling Expertise Decision Support Automation
- Incident Management Taxonomy/Ontology

## Process Improvement

- Publications/Guides
- CSIRT Toolkit

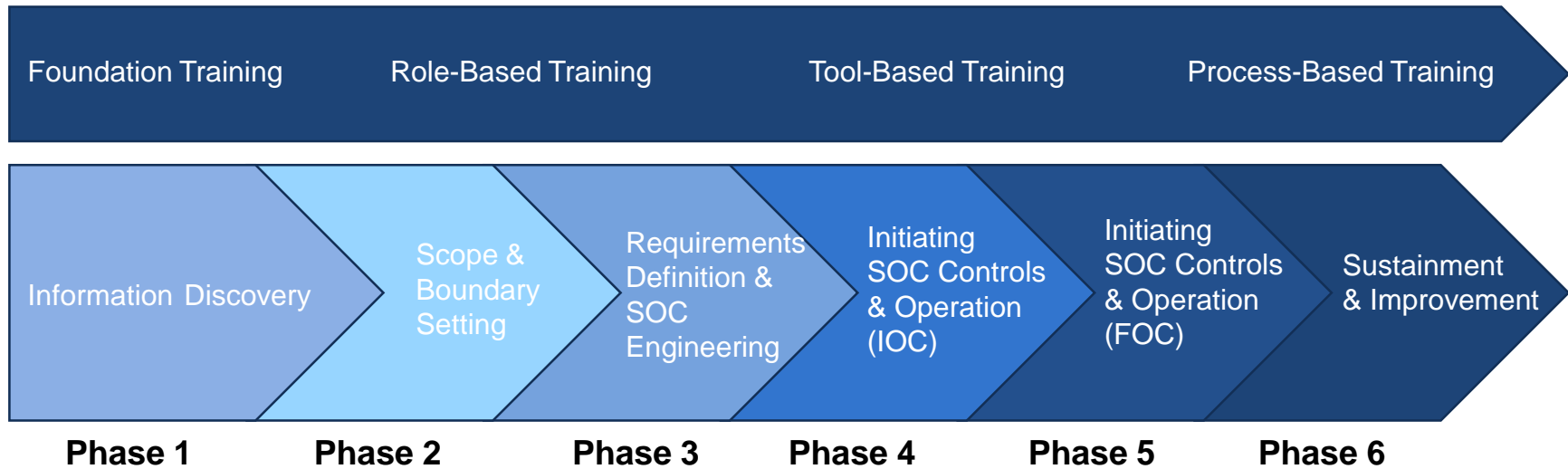
## Building Reference Models

- SOC Framework
- Incident Management Process model

## National Level Strategy & Policy Development

- International Forums
- CERT Trademark Process
- Recommendations, As Requested

# SOC Design Methodology



# Security Operations Reference Model



## Currently defining

- Terms
- Components
- Interfaces
- Workflows

## Deliverables

- Two courses
  - Security Operation Center (SOC) Concepts and Practices
  - Effective Security Operations
- Whitepapers
- Reference Model
- Assessments
- Tailored Training & Mentoring
  - Design
  - Strategic roadmaps
  - Operations and processes artifacts
  - Tool evaluation
  - Best practices

# SOC Framework and Development

- The SEI provides expertise in SOC best practices, to include assistance with:
  - Defining SOC roles and responsibilities
  - Developing SOC strategies, processes, CONOPs
  - Tailoring SOC design to address organizational strategy, goals, and challenges
  - Building situational awareness and structured analysis
- Training, courses, and roadmap development can be tailored to:
  - Individuals performing SOC roles and activities
  - Individuals coordinating or interfacing with the SOC
  - Organizations who are building, benchmarking, or looking to improve their SOC processes
  - Individuals who are high level executives wanting to better understand SOC operations and improvements

# Contact Information

Kristopher Rush

Technical Director, Monitoring and Response Directorate

Telephone: +1 412.268.9239

Email: [krush@cert.org](mailto:krush@cert.org)

James Lord

Security Operations Technical Manager

Telephone: +1 412.268.3945

Email: [jclord@cert.org](mailto:jclord@cert.org)

Michael Massa

Program Manager

Telephone: +1 703.247.1333

Email: [mdmassa@cert.org](mailto:mdmassa@cert.org)