Incident Management Overview

Foundations of Incident Management (FIM)

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Notices

This material is based upon work funded and supported by the Independent Agency 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 sponsored by the United States Department of Defense.

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.

DM19-0875

Purpose

To discuss the current state of the intruder threat to computer security

To define the nature and purpose of incident management and CSIRTs

To review the various processes associated with incident management

To provide insight into activities and tasks performed by incident handlers and CSIRT staff

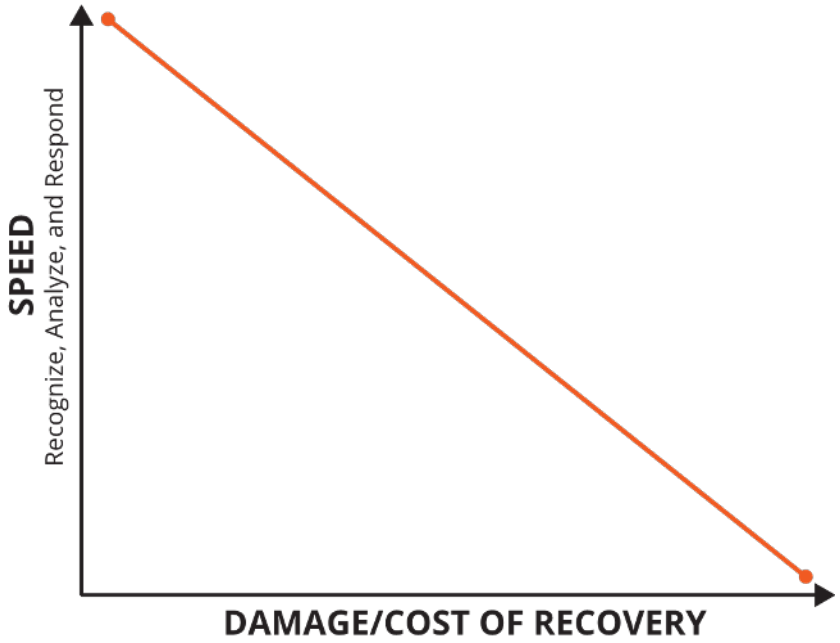
To discuss current trends and issues related to incident handling

Defining Incident Management (IM)

Effective Incident Management Leads to Better Operational Resilience

Having a better response process in place enables a higher level of operational resilience.

Framing the Problem

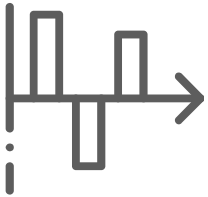


The speed with which an organization can recognize, analyze, and respond to an incident limits the damage done and lowers the cost of recovery.

Strategies for Effective Response

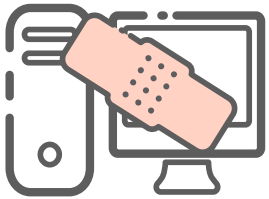
Organizations require a multi-layered approach to secure and protect their critical assets and infrastructures.

Identify Key Assets

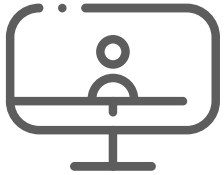


Perform Risk Assessments

Install Defenses

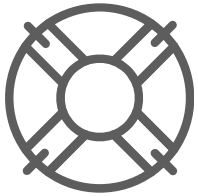


Keep System Patched



Provide Security Training

Install Defenses



Formalize Incident Management Process

In-class Discussion: Incident

What is an incident

- in general?
- specifically for your organization?

Incident Definitions

IT Infrastructure Library (ITIL) 2011

- an unplanned interruption to an IT Service or reduction in the quality of an IT service

ISO/IEC 27035-1:2016

- single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

SANS Computer Security Incident Handling Step-by-Step Guide

- “an adverse event in an information system and/or network, or the threat of the occurrence of such an event”

NIST Computer Security Incident Handling Guide

- “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices”

In-class Discussion: Incident Management

What is incident management

- in general?
- specifically for your organization?

What Do Others Say?

CERT-RMM: Incident Management and Control

- The purpose of Incident Management and Control is to establish processes to identify and analyze events, detect incidents, and determine an appropriate organizational response.

Business Dictionary

- activities a company uses to identify, classify, investigate, and repair hazards, hazardous situations, and crisis events

IT Infrastructure Library (ITIL)

- The process responsible for managing the lifecycle of all incidents. The primary … to return the IT Service to Users as quickly as possible.

DigitalGuardian

- Security incident management is the process of identifying, managing, recording and analyzing security threats or incidents in real-time.

ISO/IEC 27035-1:2016 Principles of Incident Management

The incident management process is described in five phases:

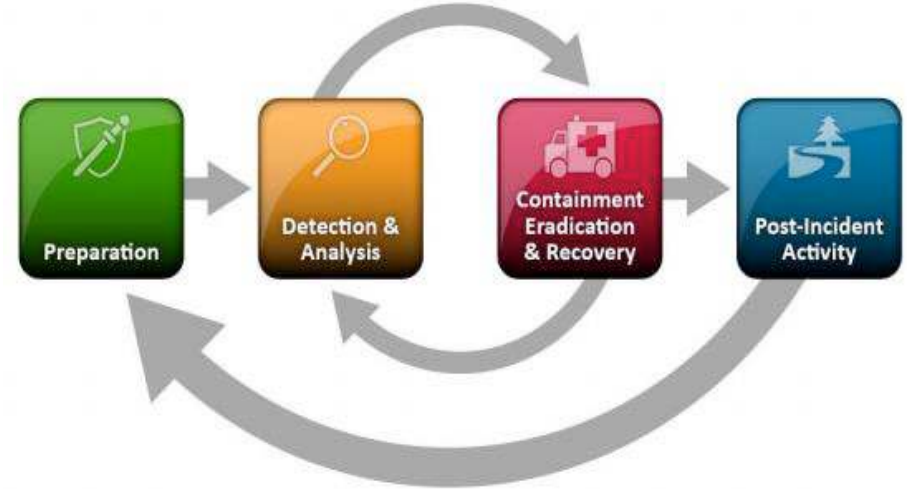
- Plan and prepare: establish an information security incident management policy, form an Incident Response Team, etc.
- Detection and reporting: someone has to spot and report “events” that might be or turn into incidents.
- Assessment and decision: someone must assess the situation to determine whether it is in fact an incident.
- Responses: contain, eradicate, recover from and forensically analyze the incident, where appropriate.
- Lessons learned: make systematic improvements to the organization’s management of information risks as a consequence of incidents experienced.

Source: https://www.iso27001security.com/html/27035.html

Incident Management Definition

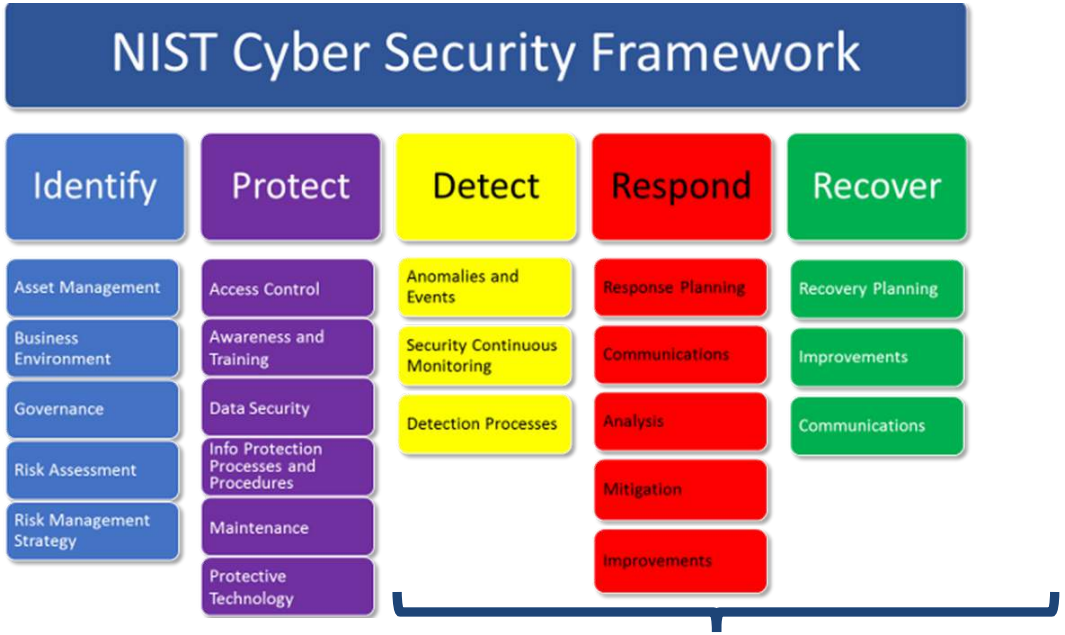
The actions the organization takes to prevent or contain the impact of an incident to the organization while it is occurring or shortly after it has occurred.

Several Phases (*NIST SP 800-61R2*)

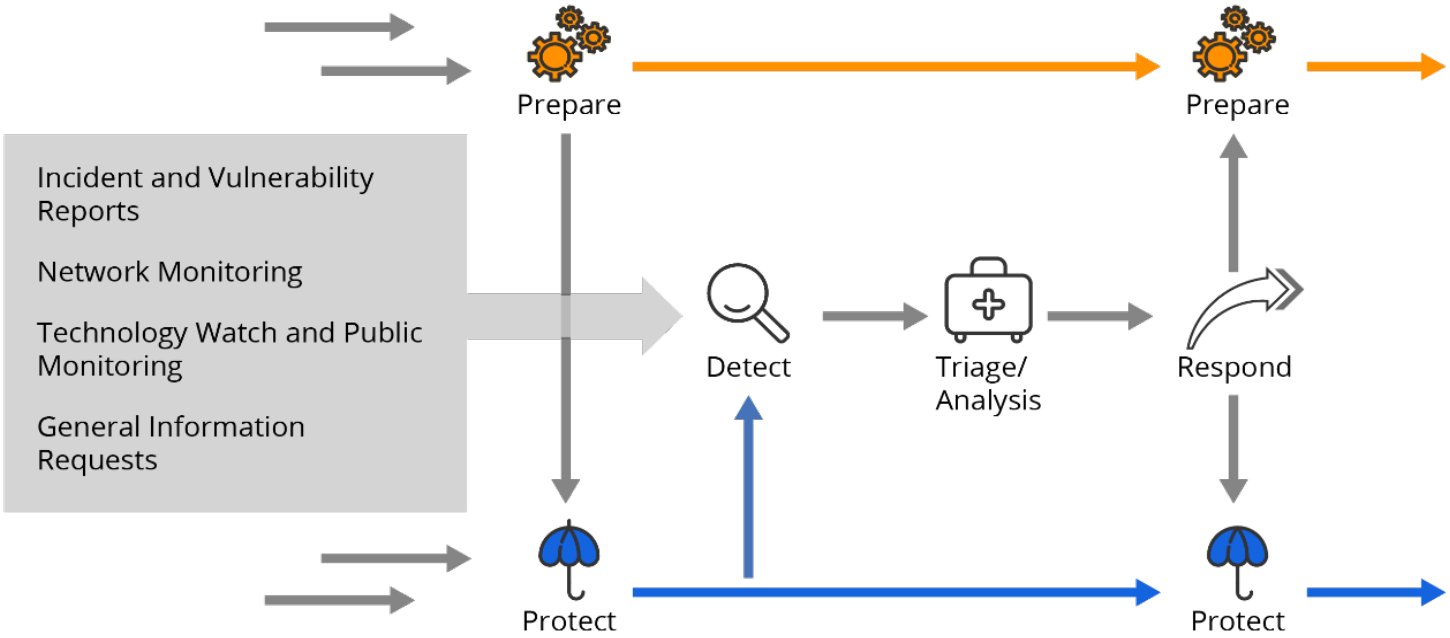


Incident Management Does Not Stand Alone

Incident Management is part of Cybersecurity Assurance or Information Security Operations Framework.



Incident Management Process Model



In-class Discussion: Incident Handling

What is incident handling?

- in general?
- specifically for your organization?

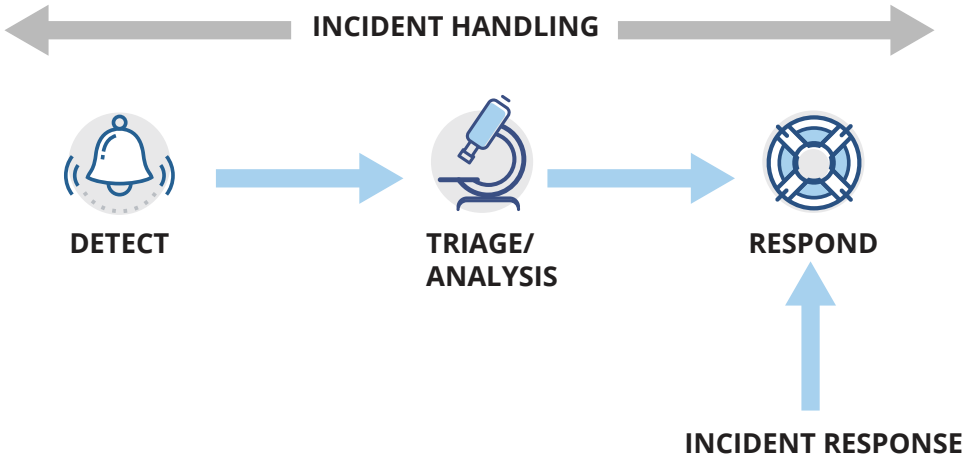
What Is Incident Handling?

It is a collection of services related to the management of a cyber-event, including alerting constituents and coordinating activities associated with the detection, analysis, response, mitigation, and recovery from an incident.

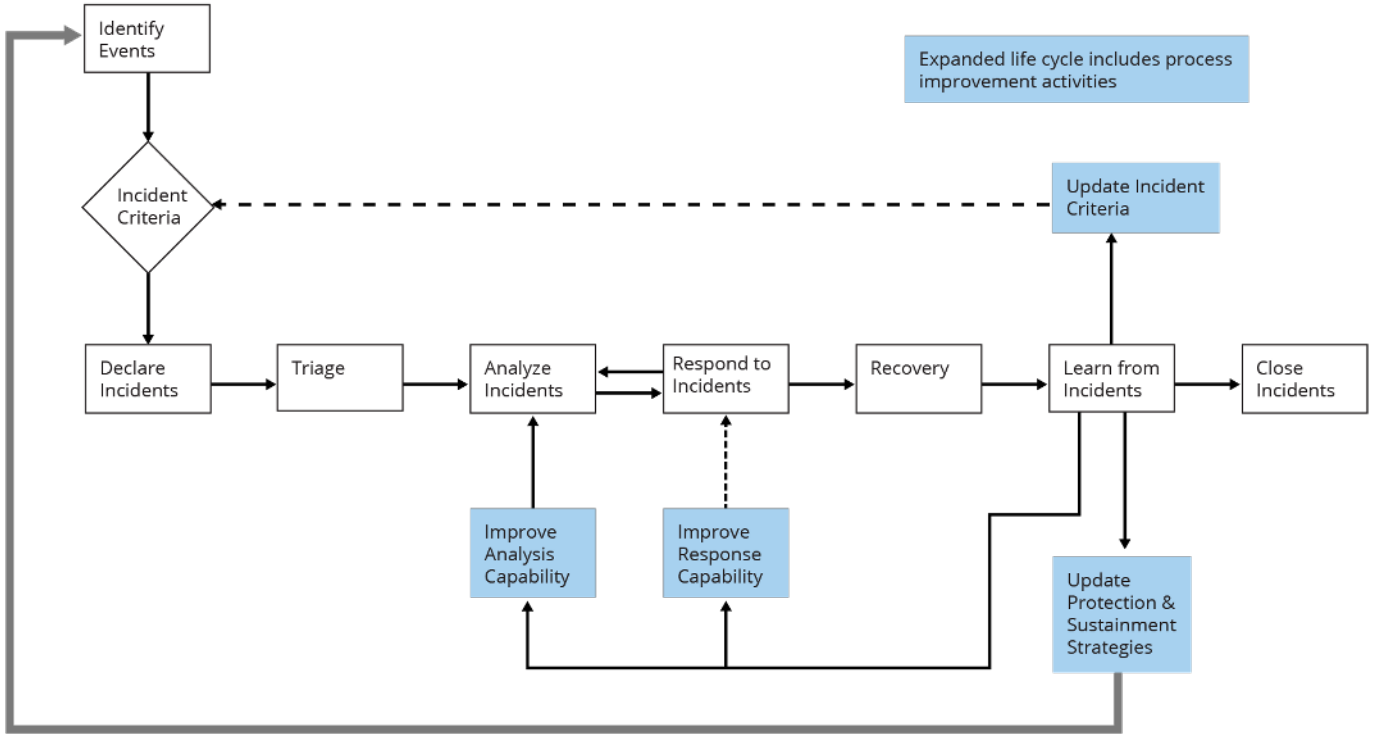
Defining the Terms

What are the definitions, and what are the differences?

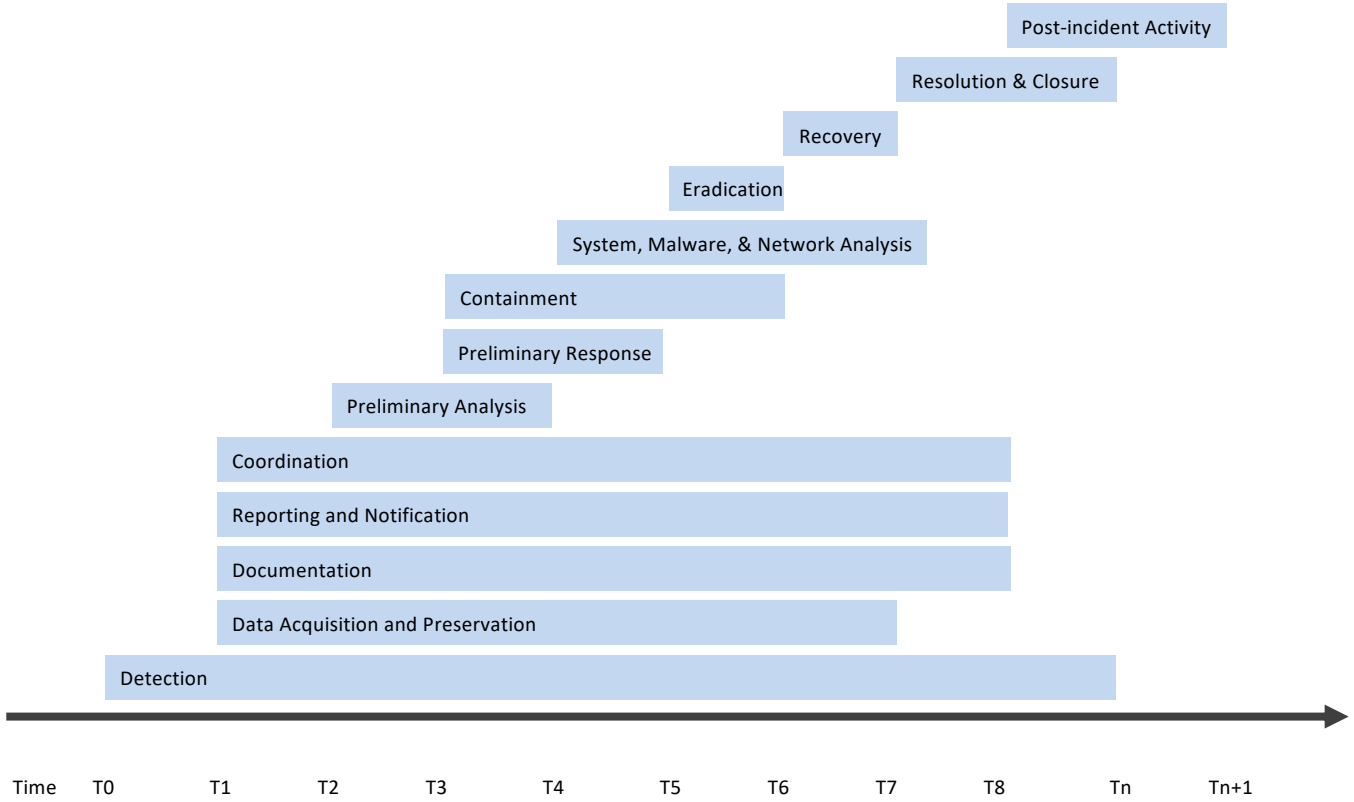
- incident management
- incident handling
- incident response



Incident Handling Process

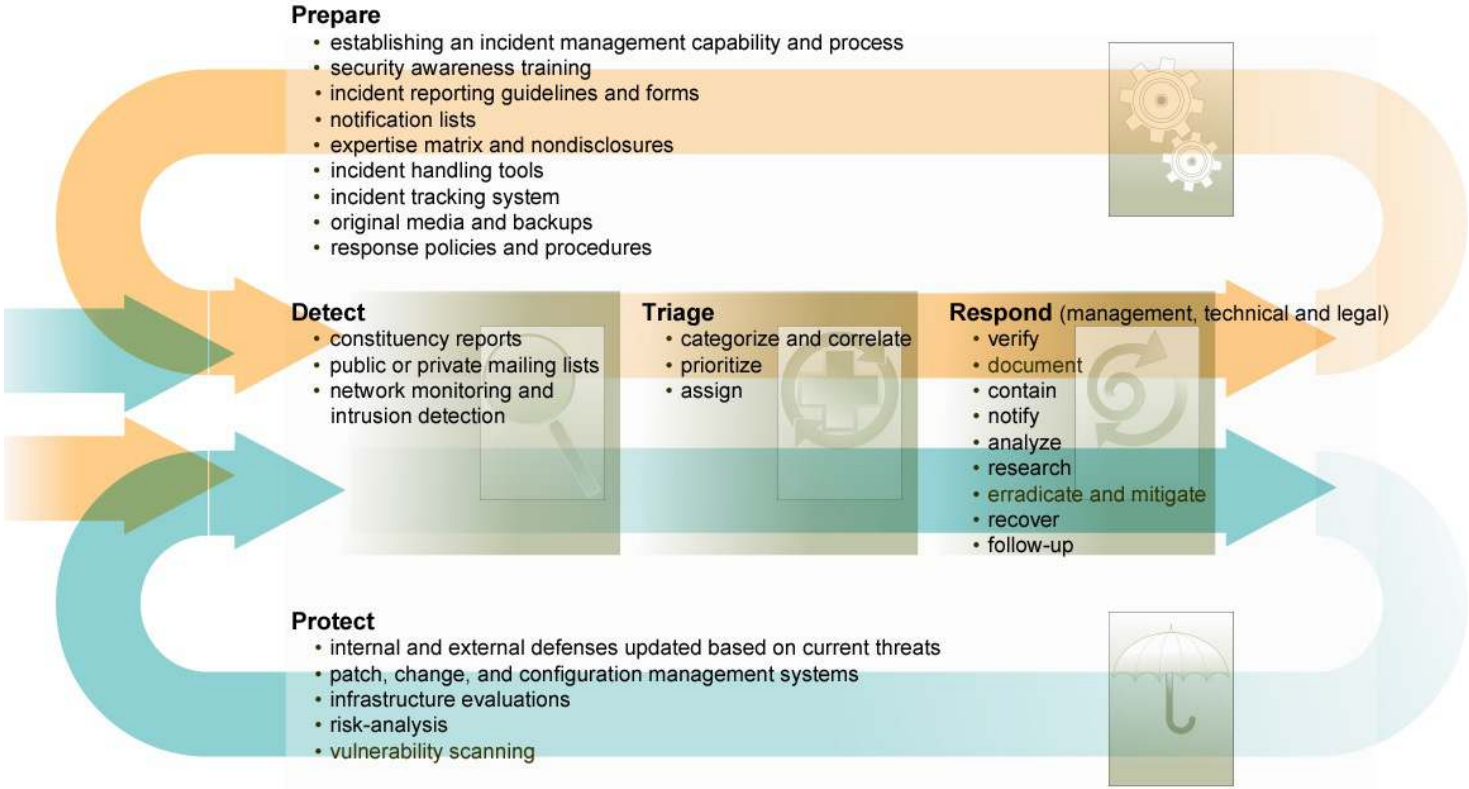


Importance of Documentation and Coordination



Incident Management Activities and Functions

Incident Management Starts Before an Incident Occurs



What's in Your Incident Management Plan?

Effective incident management requires having a formalized and institutionalized plan.

- mission and scope
- authority
- roles and responsibilities
- basic incident handling steps
- defined workflows and interfaces
- service or function descriptions
- escalation path
- communication and notification processes
- related documents and guidance
- reporting guidance

What Supports Your Incident Management Plan?

Governance support of incident management plan

Recognition of the importance of incident management

Risk analysis and resulting output

Information classification scheme

Incident criteria
- definition of incident
- prioritization
- categorization
- escalation

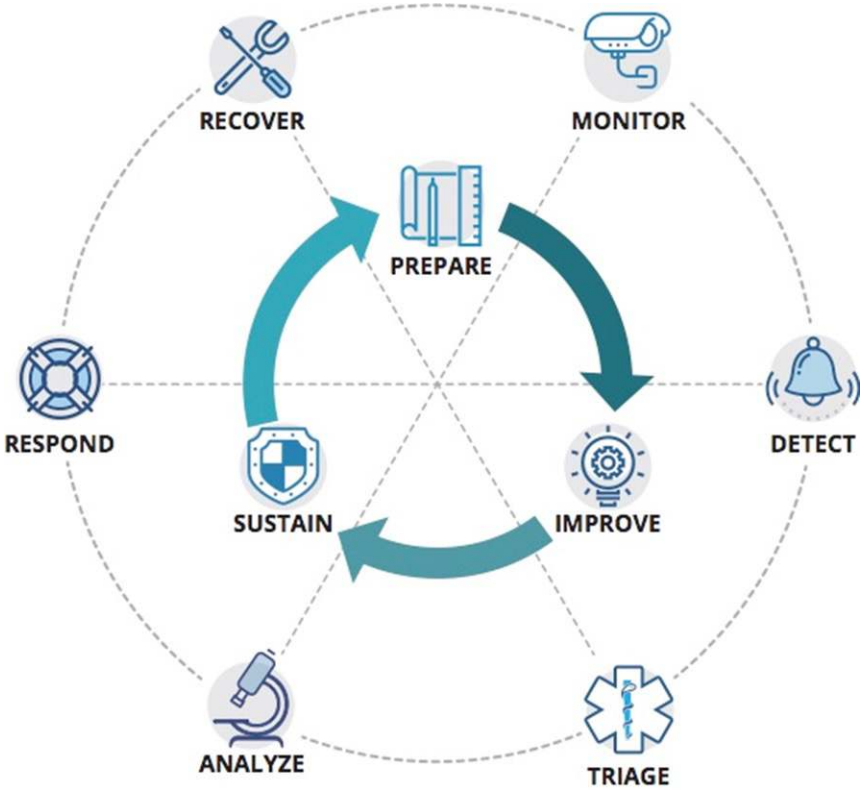
Incident reporting policy, guidelines and reporting template

Incident playbooks

Critical systems and data inventories

Guidelines for handling Personally Identifiable Information (PII)

Incident Management Lifecycle



Preparation

Goal

- effective and efficient incident management through preparation and prevention

Approach

- Integrate with risk management and information assurance activities.
- Establish capability.
- Define processes and procedures.
- Define interfaces and coordination.
- Organize tools and resources.
- Establish baselines.
- Establish incident criteria.

Preparation: Incident Prevention

Security controls
- host and network

Risk assessment
- system and asset inventory
- critical or high value assets identified
- vulnerability critical path

Awareness and training
- organizational security policies
- acceptable use
- incident reporting
- changes in policy

Detect

Detect

Goal

- accurate detection and analysis of incidents

Approach

- manual and automated data analysis

Detection

- sensing
- data
- established methods for data collection and analysis

Triage

Triage

Categorize

Prioritize

Correlate

Assign for handling

Analysis

Analyze

Validate

- Determine if the incident is REAL.
- Identify the facts of the incident.

Analyze

- Examine collected evidence.
- Look for corroboration within supporting data sources (logs, network traffic, etc.).
- Investigate incident cause, method, and outcome.

Document

- Record the facts of the incident.
- Update during incident lifecycle.

Prioritize

- operational impact

Notify

- leadership
- owners and maintainers

Evidence Gathering and Handling – Supports Analysis

Analyze

Primary purpose
- incident resolution

Secondary purpose
- legal proceedings

Preserve evidence as appropriate.
- detailed log
- chain of custody

Details
- personnel
- date/time
- locations

Identifying Hosts – Supports Analysis

Analyze

Primary purpose

- support incident response process

Secondary purpose

- intelligence collection and reporting

Validate incident hosts.

- internal
- external

Sources

- public
- private

Respond: Containment, Eradication, and Mitigation

Respond

Goals

- maintain business operations
- limit damage
- restore operations

Approach

- detection and analysis combined with enterprise collaboration, coordination, and execution

Evidence gathering and handling

Identifying hosts

Containment

Eradication

Resolution / Mitigation

Recovery


Recover

Goal
- reduce attack surface
- remediate affected systems and accounts

Requires enterprise coordination
- security, infrastructure, operations

Phased approach
- high-value changes first
- strategic changes follow

Post-Incident Activity Phase

Improve

Goal

- learn and improve from previous incidents

Approach

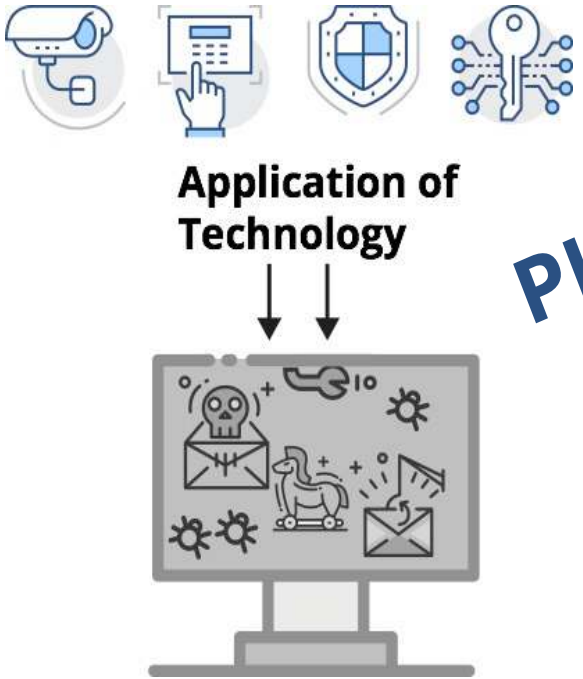
- review what occurred, what was done to respond, and how well response worked

Lessons learned

Reporting

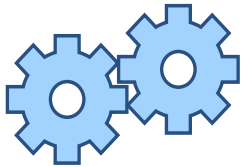
Evidence retention

Technology Versus Process



PLUS

Action Plan



Processes Set

- consistent
- repeatable
- quality driven
- measurable
- understood

Institutionalizing Incident Management

Who Performs Incident Management?

Incident management functions could be performed by

- CSIRT staff and manager
- IT staff
- physical security staff
- subject matter experts
- vendors
- ISPs/network service providers
- members of the CSIRT constituency
- victims or involved sites
- other CSIRTs or coordination centers
- upper management
- business function units
- HR staff
- PR staff
- auditors, risk management staff, compliance staff
- legal counsel for constituency or CSIRT
- inspector generals
- attorney generals
- law enforcement
- criminal investigators
- forensics specialists
- managed service providers

Institutionalizing Incident Management Capabilities -1

Some organizations may perform this function as part of other security, IT, risk management, or business continuity functions.

- common in commercial industry or the military, where this function may be served by
  - security operation centers (SOCs)
  - network operation centers (NOCs)
  - combined network and security operation centers (NSOCs)
  - security response teams
  - crisis management teams
  - resilience teams

Some organizations may outsource this capacity.

Institutionalizing Incident Management Capabilities -2

There may also be various ways an incident management capability is organized.

It may be

- a stand alone organization
- a specialized or expert group within a SOC or IT organization
- a virtual matrixed expert group pulled from various organizational areas and functions
- an expert group within a tiered call center or helpdesk, usually a Tier 3 or higher

Institutionalizing Incident Management Capabilities -3

Some organizations may assign responsibility for this function to a defined group of people or a designated unit such as a computer security incident response team or CSIRT.

This can be seen in organizations such as

- national initiatives
- local, state, or provincial governments
- educational institutions or research networks

Defining Computer Security Incident Response Teams (CSIRTs)

What Is a CSIRT?

An organization or team that provides services and support, to a defined constituency, for ***preventing***, ***handling*** and ***responding*** to computer security incidents

What Does a CSIRT Do?

In general a CSIRT

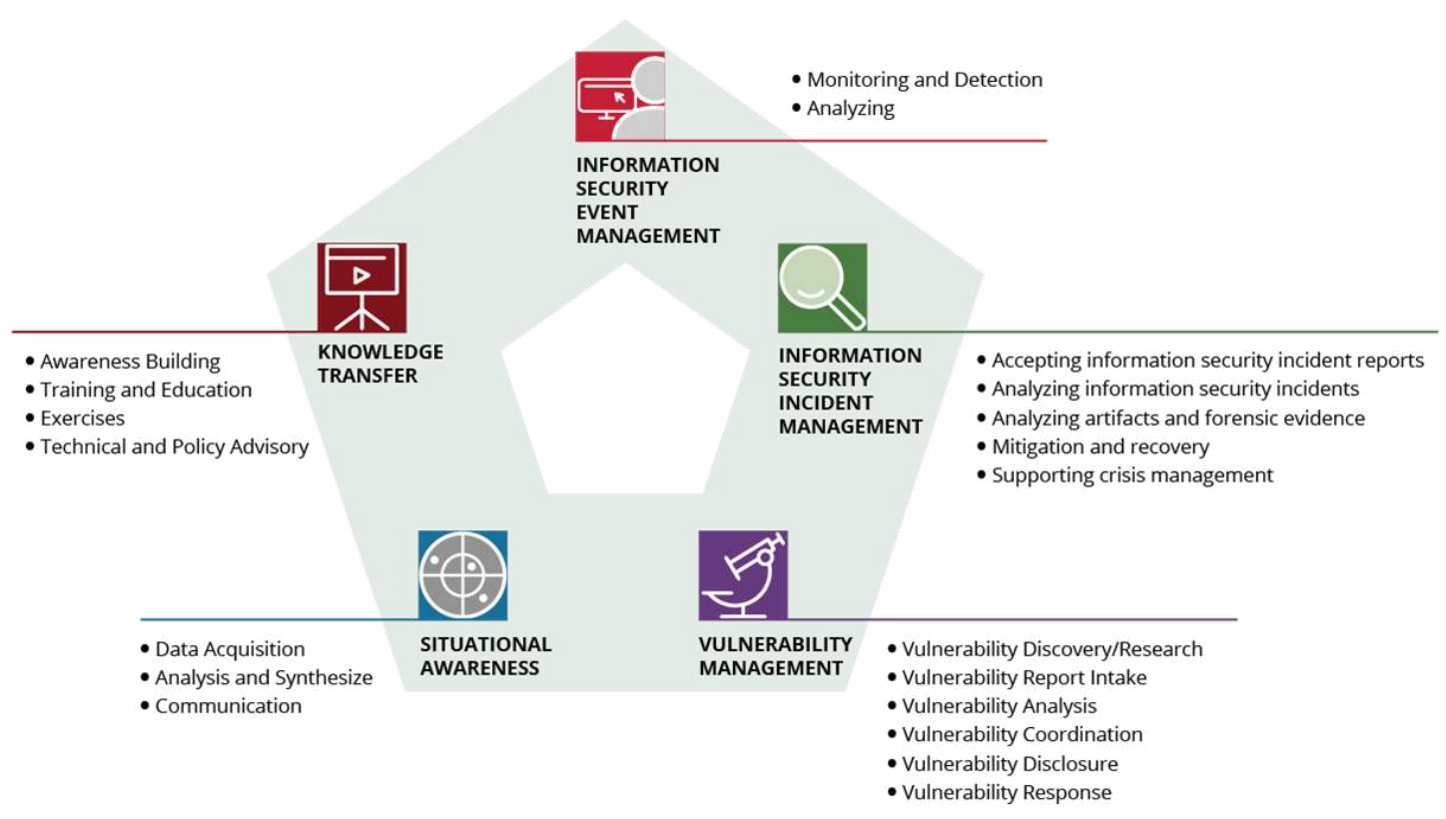
- provides a single point of contact for reporting local problems
- identifies and analyses what has happened including the impact and threat
- researches solutions and mitigation strategies
- shares response options, recommendations, incident information, and lessons learned
- coordinates the response efforts

A CSIRT's goal is to

- minimize and control the damage
- provide or assist with effective response and recovery
- help prevent future events from happening

No single team can be everything to everyone!

Draft CSIRT Services Framework 2.0



Types of CSIRT Roles

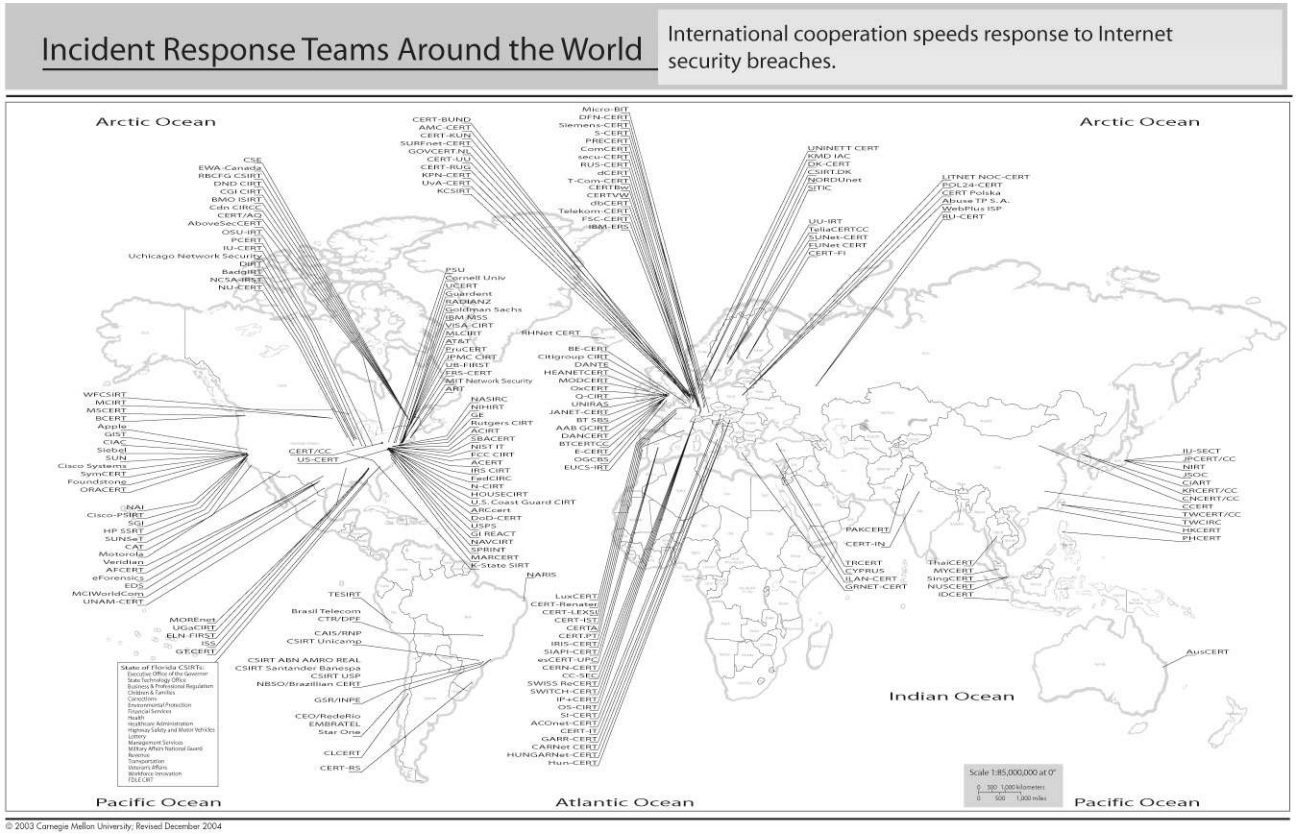
Core Staff

- manager or team lead
- assistant managers, supervisors, or group leaders
- incident handlers
- vulnerability handlers
- artifact analysis or malicious code analysis staff
- forensic analysts
- network monitors, analysts, or auditors
- hotline, help desk, or triage staff
- technology watch/public monitors
- platform and application specialists
- trainers

Extended Staff

- support staff
- technical writers
- network or system administrators for CSIRT or constituency infrastructure
- programmers or developers (to build CSIRT or security tools)
- physical security and information security staff
- web developers and maintainers
- media relations
- legal or paralegal staff or liaison
- law enforcement staff or liaison
- auditors or quality assurance staff
- marketing staff
- human resources

Variety of CSIRTs Across the Globe



Types of CSIRTs

Internal / Organizational Teams

National CSIRTS

Regional CSIRTs

Product Security Incident Response Teams (PSIRTs)

Coordination Centers / Cyber Security Centers

Information Sharing and Analysis Centers

Management Service Providers – Incident Response Providers

National CSIRT Initiatives

Various countries have established national CSIRTs.

National CSIRTs have responsibility for a country or economy.

They can serve different constituencies:

- government organizations
- critical infrastructures
- the public in general
- others

The goals of national initiatives can include

- establishing a focal point for incident coordination
- facilitating communications across diverse sectors
- developing mechanisms for trusted communications

National CSIRT Examples

U.S. Computer Emergency Readiness Team (US-CERT)

https://www.us-cert.gov/

Computer Emergency Response Team Brazil (CERT.br)

https://www.cert.br/

Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

https://www.jpcert.or.jp/english/

Q-CERT, Qatar's Center for Information Security

https://qcert.org/

Regional Initiatives

Various areas have set up regional CSIRT initiatives.

- TF-CSIRT in Europe
- APCERT in the Asia Pacific area

These initiatives involve creating an organizational entity for participation by CSIRTs within a geographic area.

These organizational entities

- are usually voluntary in nature
- can provide services or support to participating CSIRTs
- allow teams sharing similar legislative, cultural, and time zone issues to collaborate and coordinate incident handling activities

Lists of CSIRTs

Links to other CSIRT teams

- Forum of Incident Response and Security Teams (FIRST)
  https://www.first.org/members/teams/
- European CSIRT Directory
  https://www.trusted-introducer.org/directory/
- Asia Pacific Computer Emergency Response Team
  https://www.apcert.org/about/structure/members.html
- AfricaCERT – Countries
  https://www.africacert.org/home/countries/
- Lacnic (Latin American Countries)
  https://csirt.lacnic.net/en
- CERT® List of National CSIRTs
  https://www.cert.org/incident-management/national-csirts/national-csirts.cfm

Summary

Impact on CSIRTs

Today's dynamic and integrated environment means less time for CSIRTs to react and the need for more interaction, communication, and data sharing.

Therefore, teams require

- a method for quick notification
- established and understood policies and procedures
- automation of incident handling tasks
- methods to collaborate and share information with others
- easy and efficient ways to sort through and correlate all incoming information
- tools to display real-time network and system status
- assistance in preventing attacks from occurring

The Life of an Incident Handler -1

Tasks and actions performed by an incident handler

- monitoring system and network logs
- analyzing reports to determine
  - impact
  - scope and magnitude
  - involved sites
  - methods of attack
  - trends in intruder activities
- analyzing corresponding logs and files such as
  - sniffer, firewall, or router logs
  - UNIX syslogs or Windows auditing logs
  - intruder files and artifacts
  - exploit scripts
- researching involved site or host information to
  - identify hostnames / IP addresses
  - determine site contact information
- containment and eradication of threats
- providing direct technical assistance through
  - on-site assistance
  - telephone response
  - email response
  - email auto-responder
  - web or hardcopy documents

The Life of an Incident Handler -2

- coordinating and sharing information
  - developing and disseminating alerts, advisories, and notifications
  - facilitating communications and collaborating with other parts of the enterprise, other sites, other CSIRTs, law enforcement, and management
  - mailing information to involved sites
  - encrypting and decrypting sensitive information
  - receiving and storing logs, exploits, and files
  - tracking tasks and actions
  - contacting vendors
  - preparing reports, statistics, and briefings
- performing other duties as required
  - preparing for media inquiries
  - assessing time and resources used and damage incurred
  - working with law enforcement or investigation organizations to collect and secure evidence following chain of custody rules and practices
  - supporting prosecution activity and acting as expert witnesses (if appropriate)
  - supporting activities to notify victims of unauthorized release of personal data

Needed Tools, Techniques, and Skills

Understanding

- network concepts and fundamentals
- defense-in-depth strategies
- intruder exploits and attacks
- mitigation and containment strategies
- new tools such as
  - Data Execution Prevention (DEP)
  - Address Space Layout Randomization (ASLR)

Being able to perform

- packet capture analysis
- netflow analysis
- surface and runtime analysis
- forensics evidence collection and analysis
- signature development
- data analysis, correlation, and visualization
- incident containment, response, and coordination

Along with understanding

- risk management concepts and techniques
- enterprise and mission focus
- policy impact
- project management concepts and techniques

Being able to perform

- business and operational impact analysis
- trend analysis
- situational awareness data collection

And being a

- team player
- good communicator and collaborator

CSIRTs Are Customer-service Focused

CSIRTs still need to continue focusing on

- communicating with stakeholders and collaborators
- developing trusted relationships
- coordinating detection, analysis, and response efforts
- finding ways to share meaningful and actionable information in a secure and timely manner
- finding better faster methods of detection and response
- helping others find better ways for developing secure software and methods of prevention
- providing awareness and training
- obtaining practical experience through coordinated cyber exercises

Management Issues Review

As an incident handler you may focus on technical analysis and solutions, but to be ***effective*** you have to understand some organizational and management issues.

- What are the ***critical services*** and ***data*** that need to be ***protected*** in your organization or constituency?
- What is your ***mission***?
- What ***role*** do you play in the organization or constituency?
- How does your work ***interface*** with other parts of your organization or constituency?

Novice vs. Mature Teams

Our experiences have shown that generally new teams

- need time to establish relationships with constituents, stakeholders, and collaborators
- end up focusing on more reactive versus proactive services
- have less well defined interfaces and procedures

While more mature teams generally

- have documented processes, policies, and procedures
- have well defined interfaces and communication channels
- have instituted and enforced a training and mentoring plan
- have a quality assurance program in place
- have an evaluation mechanism in place to measure their success
- participate in more collaboration and data sharing activities
- balance between reactive and proactive services
- provide input into quality management services
- understand their stakeholder's needs and work with them in a collaborative manner
- focus on a more enterprise view – involving a variety of stakeholders

Novice vs. Mature Teams

Our experiences have shown that

Generally, new teams

- need time to establish relationships with constituents, stakeholders, and collaborators
- end up focusing on more reactive versus proactive services
- have less well defined interfaces and procedures

While more mature teams, generally

- have documented processes, policies, and procedures
- have well defined interfaces and communication channels
- have instituted and enforced a training and mentoring plan
- have a quality assurance program in place
- have an evaluation mechanism in place to measure their success
- participate in more collaboration and data sharing activities
- balance between reactive and proactive services
- provide input into quality management services
- understand their stakeholder's needs and work with them in a collaborative manner
- focus on a more enterprise view – involving a variety of stakeholders

Resources

Incident Handling Resource Sites

CERT Coordination Center
https://www.cert.org/

United States Computer Emergency Readiness Team
https://www.us-cert.gov/

Forum of Incident Response and Security Teams
https://www.first.org/

The SANS (SysAdmin, Audit, Network, Security) Institute
https://www.sans.org/

European Union Agency for Network and Information Security (ENISA)
https://www.enisa.europa.eu/

CSIRT Maturity Kit
https://check.ncsc.nl/static/CSIRT_MK_guide.pdf

CERT Resources That Can Help

CERT CSIRT Publications

- Handbook for CSIRTs, Second Edition
  https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305
- Defining Incident Management Processes for CSIRTs:
  A Work in Progress
  https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153
- Organizational Models for CSIRTs
  https://resources.sei.cmu.edu/asset_files/handbook/2003_002_001_14099.pdf
- State of the Practice of CSIRTs
  https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6571
- Staffing Your Computer Security Incident Response Team – What Basic Skills are Needed?
  https://resources.sei.cmu.edu/asset_files/whitepaper/2017_019_001_485684.pdf#
- Action List for Developing a Computer Security Incident Response Team (CSIRT)
  https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=53102

Other Resources: ENISA

The European Union Agency for Network and Information Security (ENISA) has various publications and artifacts including

- community information and documents
  - financial
  - SCADA
  - energy
  - law enforcement
- training resources, exercises include
  - legal & cooperation
  - setting up a CSIRT
  - operational
  - technical
- cyber crisis management

Other Resources: Team Cmyru

General Information and Public Services

https://www.team-cymru.org/Services/

- The Bogon Reference
- The Darknet Project
- The IP to ASN Mapping Project
- The Malware Hash Registry
- Totalhash Malware Analysis

CSIRT Assistance Program

https://team-cymru.com/community-services/#

will partner with Regional and National CSIRTs

- small set of conditions to apply (like MOU)

To join the program, send an email with the subject “CSIRT Assistance Program” to outreach@cymru.com.

Other Resources: CERT.br

CERT.br

- https://www.cert.br/projects/
- Honeypots
  - will report to the National CSIRT activity in your region
  - provides public statistics
    - daily https://honeytarg.cert.br/honeypots/stats/flows/current/
    - hourly portscan
    - https://honeytarg.cert.br/honeypots/stats/portsum/24-hour/current/
- SpamPots Project
  - https://honeytarg.cert.br/spampots/
  - currently deployed in 9 countries to compare spam traffic
    - Australia, Austria, Chile, Uruguay, Brazil, Ecuador, Netherlands, Taiwan, and the United States
  - Your team could join this project and share the information.

Other Resources: Honeynet

Honeynet Project: https://www.honeynet.org/

- uses various systems/tools that often simulate vulnerable systems that can be compromised easily
- allows for easy monitoring of the system
- broken up by chapters that work together to collect and share information seen on their systems: https://www.honeynet.org/category/chapters/

CSIRT Related Initiatives -1

Global Forum on Cyber Expertise launched April 2015 – initiatives:

- CSIRT Maturity
- Responsible Disclosure
- Cyber Security awareness raising

Internet Governance Forum (IGF) – Best Practice Forum (BPF) CSIRTs

- Mailing list discussions
- Yearly projects, final work presented at IGF

  https://mail.intgovforum.org/mailman/listinfo/bp_certs_intgovforum.org

FIRST Special Interest Groups (SIGs)

- CSIRT Metrics
- Ethics and Privacy
- Cyber Threat Intelligence
- Common Vulnerability Scoring System (CVSS)
- Vulnerability Reporting and Data Exchange
- Vulnerability Coordination
- Big Data
- Cyber Insurance
- Red Team
- Product Security Incident Response Teams (PSIRTs)
- And many more

CSIRT Related Initiatives -2

Institute for Information Infrastructure Protection (I3P)

- Improving CSIRT Skills, Dynamics, and Effectiveness (3 year project) https://www.thei3p.org/
- Organization for Economic Co-operation and Development
- Improving the international comparability of Computer Security Incident Response Teams statistics https://www.oecd.org/sti/ieconomy/informationsecurityandprivacyindicators.htm

Global Cyber Security Capacity Center, Oxford Martin School

- Improving the effectiveness of CSIRTs https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Improving%20the%20effectiveness%20of%20CSIRTs.pdf

Key Points

Computer security threats and risks continue to evolve: they are more complex, sophisticated, and cause real damage.

CSIRTs and incident management capabilities come in all varieties; their mission and goals should match the goals of their parent organization or constituency.

Incident Management requires the establishment of processes for

- notification and communication
- collaboration and coordination
- analysis and response
- documentation and tracking

The CSIRT community provides mechanisms for information sharing, collaboration, and coordination.

Q