

CSIRT Services

Introduction

One of the primary issues to be addressed in creating a computer security incident response team (CSIRT) is deciding what services the CSIRT will provide to its constituency. This process also involves naming and defining each provided service, which is not always an easy task. Experience has shown that there is often great confusion about the names used for CSIRT services. The purpose of this document is to present a list of CSIRT services and their definitions.¹ This list provides a common framework for a consistent and comparable description of CSIRTs and their corresponding services.

Although this document focuses on services provided by CSIRTs, many of these same services can also be provided by system, network, and security administrators who perform ad hoc incident handling as part of their normal administrative work when there is no established CSIRT. We refer to this type of ad hoc team as a “security team.” The enclosed service definitions can also be used by any of these organizational teams or others in the computer security field.

A CSIRT must take great care in choosing the services it will offer. The set of services provided will determine the resources, skill sets, and partnerships the team will need to function properly. The selection of services should first and foremost support and enable the business goals of the CSIRT’s constituency or parent organization. The services provided should be those that the team can realistically and honestly provide based on the team size and range of expertise. It is better to offer a few services well than a large range of services poorly. As a CSIRT gains the trust and respect of its constituency, it can look to expand its services as staff and funding permit.²

Service Categories

There are many services that a CSIRT can choose to offer. Each CSIRT is different and provides services based on the mission, purpose, and constituency of the team. Providing an incident handling service is the only prerequisite to be considered a CSIRT.

¹ The list was originally based on the example CSIRT services on page 20 of the [Handbook for Computer Security Incident Response Teams \(CSIRTs\)](#) [1]. An extended and updated list was developed by Klaus-Peter Kossakowski in the book *Information Technology Incident Response Capabilities* [2]. When Kossakowski became involved with the [Trusted Introducer for CSIRTs in Europe](#) [3], the new list was utilized to help teams describe themselves based on established service names. In an effort to consolidate CSIRT service terminology, the Trusted Introducer service worked with the CSIRT Development Team of the CERT Coordination Center, Pittsburgh, PA, to produce this updated and more comprehensive list of CSIRT services.

² More information on selecting services can be found in the [Handbook for Computer Security Incident Response Teams \(CSIRTs\)](#)

CSIRT services can be grouped into three categories:

Reactive services. These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system. Reactive services are the core component of CSIRT work.

Proactive services. These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future.

Security quality management services. These services augment existing and well-established services that are independent of incident handling and traditionally performed by other areas of an organization such as the IT, audit, or training departments. If the CSIRT performs or assists with these services, the CSIRT’s point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. These services are generally proactive but contribute indirectly to reducing the number of incidents.

The services are listed in the following table and described in detail below.

Reactive Services	Proactive Services	Security Quality Management Services
Alerts and Warnings Incident Handling Incident analysis Incident response on site Incident response support Incident response coordination Vulnerability Handling Vulnerability analysis Vulnerability response Vulnerability response coordination Artifact Handling Artifact analysis Artifact response Artifact response coordination	Announcements Technology Watch Security Audits or Assessments Configuration and Maintenance of Security Tools, Applications, and Infrastructures Development of Security Tools Intrusion Detection Services Security-Related Information Dissemination	Risk Analysis Business Continuity and Disaster Recovery Planning Security Consulting Awareness Building Education/Training Product Evaluation or Certification

It should be noted that some services have both a reactive and proactive side. For example, vulnerability handling can be done in response to the discovery of a software vulnerability that is being actively exploited. But it can also be done proactively by reviewing and testing code to determine where vulnerabilities exist, so the problems can be fixed before they are widely known or exploited.

Service Descriptions

Reactive Services

Reactive services are designed to respond to requests for assistance, reports of incidents from the CSIRT constituency, and any threats or attacks against CSIRT systems. Some services may be initiated by third-party notification or by viewing monitoring or IDS logs and alerts.

Alerts and Warnings

This service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of action for dealing with the resulting problem. The alert, warning, or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected. Information may be created by the CSIRT or may be redistributed from vendors, other CSIRTs or security experts, or other parts of the constituency.

Incident Handling

Incident handling involves receiving, triaging,³ and responding to requests and reports, and analyzing incidents and events. Particular response activities can include

- taking action to protect systems and networks affected or threatened by intruder activity
- providing solutions and mitigation strategies from relevant advisories or alerts
- looking for intruder activity on other parts of the network
- filtering network traffic
- rebuilding systems
- patching or repairing systems
- developing other response or workaround strategies

Since incident handling activities are implemented in various ways by different types of CSIRTs, this service is further categorized based on the type of activities performed and the type of assistance given as follows:

Incident analysis. There are many levels of incident analysis and many sub-services. Essentially, incident analysis is an examination of all available information and supporting evidence or artifacts related to an incident or event. The purpose of the analysis is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident, and available response strategies or workarounds. The CSIRT may use the results of vulnerability and artifact analysis (described below) to understand and provide the most complete and up-to-date analysis of what has happened on a specific system. The CSIRT correlates activity across incidents to determine any interrelations, trends, patterns, or intruder signatures. Two sub-services that may be done as part of incident analysis, depending on the mission, goals, and processes of the CSIRT, are

³ Triaging refers to the sorting, categorizing, and prioritizing of incoming incident reports or other CSIRT requests. It can be compared to triage in a hospital, where patients who need to be seen immediately are separated from those who can wait for assistance.

- **Forensic evidence collection:** the collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise. This gathering of information and evidence must be done in a way that documents a provable chain of custody that is admissible in a court of law under the rules of evidence. Tasks involved in forensic evidence collection include (but are not limited to) making a bit-image copy of the affected system's hard drive; checking for changes to the system such as new programs, files, services, and users; looking at running processes and open ports; and checking for Trojan horse programs and toolkits. CSIRT staff performing this function may also have to be prepared to act as expert witnesses in court proceedings.
- **Tracking or tracing:** the tracing of the origins of an intruder or identifying systems to which the intruder had access. This activity might involve tracking or tracing how the intruder entered the affected systems and related networks, which systems were used to gain that access, where the attack originated, and what other systems and networks were used as part of the attack. It might also involve trying to determine the identity of the intruder. This work might be done alone but usually involves working with law enforcement personnel, Internet service providers, or other involved organizations.

Incident response⁴ on site. The CSIRT provides direct, on-site assistance to help constituents recover from an incident. The CSIRT itself physically analyzes the affected systems and conducts the repair and recovery of the systems, instead of only providing incident response support by telephone or email (see below). This service involves all actions taken on a local level that are necessary if an incident is suspected or occurs. If the CSIRT is not located at the affected site, team members would travel to the site and perform the response. In other cases a local team may already be on site, providing incident response as part of its routine work. This is especially true if incident handling is provided as part of the normal job function of system, network, or security administrators in lieu of an established CSIRT.

Incident response support. The CSIRT assists and guides the victim(s) of the attack in recovering from an incident via phone, email, fax, or documentation. This can involve technical assistance in the interpretation of data collected, providing contact information, or relaying guidance on mitigation and recovery strategies. It does not involve direct, on-site incident response actions as described above. The CSIRT instead provides guidance remotely so site personnel can perform the recovery themselves.

Incident response coordination. The CSIRT coordinates the response effort among parties involved in the incident. This usually includes the victim of the attack, other sites involved in the attack, and any sites requiring assistance in the analysis of the attack. It may also include the parties that provide IT support to the victim, such as Internet service providers, other CSIRTs, and system and network administrators at the site. The coordination work may involve collecting contact information, notifying sites of their potential involvement (as victim or source of an attack), collecting statistics about the number of sites involved, and facilitating information exchange and analysis. Part of the coordination work may

⁴ Note that "incident response" is used here to describe one type of CSIRT service. When used in team names such as "Incident Response Team," the term typically has the broader meaning of incident handling.

involve notification and collaboration with an organization's legal counsel, human resources or public relations departments. It would also include coordination with law enforcement. This service does not involve direct, on-site incident response.

Vulnerability Handling

Vulnerability handling involves receiving information and reports about hardware and software vulnerabilities;⁵ analyzing the nature, mechanics, and effects of the vulnerabilities; and developing response strategies for detecting and repairing the vulnerabilities. Since vulnerability handling activities are implemented in various ways by different types of CSIRTs, this service is further categorized based on the type of activities performed and the type of assistance given as follows:

Vulnerability analysis. The CSIRT performs technical analysis and examination of vulnerabilities in hardware or software. This includes the verification of suspected vulnerabilities and the technical examination of the hardware or software vulnerability to determine where it is located and how it can be exploited. The analysis may include reviewing source code, using a debugger to determine where the vulnerability occurs, or trying to reproduce the problem on a test system.

Vulnerability response. This service involves determining the appropriate response to mitigate or repair a vulnerability. This may involve developing or researching patches, fixes, and workarounds. It also involves notifying others of the mitigation strategy, possibly by creating and distributing advisories or alerts.⁶ This service can include performing the response by installing patches, fixes, or workarounds.

Vulnerability response coordination. The CSIRT notifies the various parts of the enterprise or constituency about the vulnerability and shares information about how to fix or mitigate the vulnerability. The CSIRT verifies that the vulnerability response strategy has been successfully implemented. This service can involve communicating with vendors, other CSIRTs, technical experts, constituent members, and the individuals or groups who initially discovered or reported the vulnerability. Activities include facilitating the analysis of a vulnerability or vulnerability report; coordinating the release schedules of corresponding documents, patches, or workarounds; and synthesizing technical analysis done by different parties. This service can also include maintaining a public or private archive or knowledgebase of vulnerability information and corresponding response strategies.

Artifact Handling

An artifact is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits.

⁵ A vulnerability is the existence of a flaw or weakness in hardware or software that can be exploited resulting in a violation of an implicit or explicit security policy.

⁶ Other CSIRTs might further redistribute these original advisories or alerts as part of their services.

Artifact handling involves receiving information about and copies of artifacts that are used in intruder attacks, reconnaissance, and other unauthorized or disruptive activities. Once received, the artifact is reviewed. This includes analyzing the nature, mechanics, version, and use of the artifacts; and developing (or suggesting) response strategies for detecting, removing, and defending against these artifacts. Since artifact handling activities are implemented in various ways by different types of CSIRTs, this service is further categorized based on the type of activities performed and the type of assistance given as follows:

Artifact analysis. The CSIRT performs a technical examination and analysis of any artifact found on a system. The analysis done might include identifying the file type and structure of the artifact, comparing a new artifact against existing artifacts or other versions of the same artifact to see similarities and differences, or reverse engineering or disassembling code to determine the purpose and function of the artifact.

Artifact response. This service involves determining the appropriate actions to detect and remove artifacts from a system, as well as actions to prevent artifacts from being installed. This may involve creating signatures that can be added to antivirus software or IDS.

Artifact response coordination. This service involves sharing and synthesizing analysis results and response strategies pertaining to an artifact with other researchers, CSIRTs, vendors, and other security experts. Activities include notifying others and synthesizing technical analysis from a variety of sources. Activities can also include maintaining a public or constituent archive of known artifacts and their impact and corresponding response strategies.

Proactive Services

Proactive services are designed to improve the infrastructure and security processes of the constituency before any incident or event occurs or is detected. The main goals are to avoid incidents and to reduce their impact and scope when they do occur.

Announcements

This includes, but is not limited to, intrusion alerts, vulnerability warnings, and security advisories. Such announcements inform constituents about new developments with medium- to long-term impact, such as newly found vulnerabilities or intruder tools. Announcements enable constituents to protect their systems and networks against newly found problems before they can be exploited.

Technology Watch

The CSIRT monitors and observes new technical developments, intruder activities, and related trends to help identify future threats. Topics reviewed can be expanded to include legal and legislative rulings, social or political threats, and emerging technologies. This service involves reading security mailing lists, security web sites, and current news and journal articles in the fields of science, technology, politics, and government to extract information relevant to the security of the constituent systems and networks. This can include communicating with other parties that are authorities in these fields to ensure that the best and most accurate information or interpretation is obtained. The outcome of this service might be some type of announcement, guidelines, or recommendations focused at more medium- to long-term security issues.

Security Audits or Assessments

This service provides a detailed review and analysis of an organization's security infrastructure, based on the requirements defined by the organization or by other industry standards⁷ that apply. It can also involve a review of the organizational security practices. There are many different types of audits or assessments that can be provided, including

- infrastructure review—manually reviewing the hardware and software configurations, routers, firewalls, servers, and desktop devices to ensure that they match the organizational or industry best practice security policies and standard configurations
- best practice review—interviewing employees and system and network administrators to determine if their security practices match the defined organizational security policy or some specific industry standards
- scanning—using vulnerability or virus scanners to determine which systems and networks are vulnerable
- penetration testing—testing the security of a site by purposefully attacking its systems and networks

Obtaining upper management approval is required before conducting such audits or assessments. Some of these approaches may be prohibited by organizational policy. Providing this service can include developing a common set of practices against which the tests or assessments are conducted, along with developing a required skill set or certification requirements for staff that perform the testing, assessments, audits, or reviews. This service could also be outsourced to a third part contractor or managed security service provider with the appropriate expertise in conducting audits and assessments.

Configuration and Maintenance of Security Tools, Applications, Infrastructures, and Services

This service identifies or provides appropriate guidance on how to securely configure and maintain tools, applications, and the general computing infrastructure used by the CSIRT constituency or the CSIRT itself. Besides providing guidance, the CSIRT may perform configuration updates and maintenance of security tools and services, such as IDS, network scanning or monitoring systems, filters, wrappers, firewalls, virtual private networks (VPN), or authentication mechanisms. The CSIRT may even provide these services as part of their main function. The CSIRT may also configure and maintain servers, desktops, laptops, personal digital assistants (PDAs), and other wireless devices according to security guidelines. This service includes escalating to management any issues or problems with configurations or the use of tools and applications that the CSIRT believes might leave a system vulnerable to attack.

⁷ Industry standards and methodologies might include Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), CCTA Risk Analysis and Management Method (CRAMM), Information Security Forum's Fundamental Information Risk Management (FIRM), Commonly Accepted Security Practices and Regulations (CASPR), Control Objectives for Information and (Related) Technology (COBIT), Methode d' Evaluation de la Vulnerabilite Residuelle des Systemes d'Informa (MELISA), ISO 13335, ISO 17799, or ISO 15408.

Development of Security Tools

This service includes the development of any new, constituent-specific tools that are required or desired by the constituency or by the CSIRT itself. This can include, for example, developing security patches for customized software used by the constituency or secured software distributions that can be used to rebuild compromised hosts. It can also include developing tools or scripts that extend the functionality of existing security tools, such as a new plug-in for a vulnerability or network scanner, scripts that facilitate the use of encryption technology, or automated patch distribution mechanisms.

Intrusion Detection Services

CSIRTs that perform this service review existing IDS logs, analyze and initiate a response for any events that meet their defined threshold, or forward any alerts according to a pre-defined service level agreement or escalation strategy. Intrusion detection and analysis of the associated security logs can be a daunting task—not only in determining where to locate the sensors in the environment, but collecting and then analyzing the large amounts of data captured. In many cases, specialized tools or expertise is required to synthesize and interpret the information to identify false alarms, attacks, or network events and to implement strategies to eliminate or minimize such events. Some organizations choose to outsource this activity to others who have more expertise in performing these services, such as managed security service providers.

Security-Related Information Dissemination

This service provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security. Such information might include

- reporting guidelines and contact information for the CSIRT
- archives of alerts, warnings, and other announcements
- documentation about current best practices
- general computer security guidance
- policies, procedures, and checklists
- patch development and distribution information
- vendor links
- current statistics and trends in incident reporting
- other information that can improve overall security practices

This information can be developed and published by the CSIRT or by another part of the organization (IT, human resources, or media relations), and can include information from external resources such as other CSIRTs, vendors, and security experts.

Security Quality Management Services

Services that fall into this category are not unique to incident handling or CSIRTs in particular. They are well-known, established services designed to improve the overall security of an organization. By leveraging the experiences gained in providing the reactive and proactive services described above, a CSIRT can bring unique perspectives to these quality management services that might not otherwise be available. These services are designed to incorporate feedback and lessons learned based on knowledge gained by responding to incidents, vulnerabilities, and attacks. Feeding such experiences into the established traditional services (described below) as part of a security quality management process can improve the long-term security efforts in an organization.

Depending on organizational structures and responsibilities, a CSIRT may provide these services or participate as part of a larger organizational team effort.

The following descriptions explain how CSIRT expertise can benefit each of these security quality management services.

Risk Analysis

CSIRTs may be able to add value to risk analysis and assessments. This can improve the organization's ability to assess real threats, to provide realistic qualitative and quantitative assessments of the risks to information assets, and to evaluate protection and response strategies. CSIRTs performing this service would conduct or assist with information security risk analysis activities for new systems and business processes or evaluate threats and attacks against constituent assets and systems.

Business Continuity and Disaster Recovery Planning

Based on past occurrences and future predictions of emerging incident or security trends, more and more incidents have the potential to result in serious degradation of business operations. Therefore, planning efforts should consider CSIRT experience and recommendations in determining how best to respond to such incidents to ensure the continuity of business operations. CSIRTs performing this service are involved in business continuity and disaster recovery planning for events related to computer security threats and attacks.

Security Consulting

CSIRTs can be used to provide advice and guidance on the best security practices to implement for constituents' business operations. A CSIRT providing this service is involved in preparing recommendations or identifying requirements for purchasing, installing, or securing new systems, network devices, software applications, or enterprise-wide business processes. This service includes providing guidance and assistance in developing organizational or constituency security policies. It can also involve providing testimony or advice to legislative or other government bodies.

Awareness Building

CSIRTs may be able to identify where constituents require more information and guidance to better conform to accepted security practices and organizational security policies. Increasing the general security awareness of the constituent population not only improves their understanding of security issues but also helps them perform their day-to-day operations in a more secure manner. This can reduce the occurrence of successful attacks and increase the probability that constituents will detect and report attacks, thereby decreasing recovery times and eliminating or minimizing losses.

CSIRTs performing this service seek opportunities to increase security awareness through developing articles, posters, newsletters, web sites, or other informational resources that explain security best practices and provide advice on precautions to take. Activities may also include scheduling meetings and seminars to keep constituents up to date with ongoing security procedures and potential threats to organizational systems.

Education/Training

This service involves providing information to constituents about computer security issues through seminars, workshops, courses, and tutorials. Topics might include incident reporting guidelines, appropriate response methods, incident response tools, incident prevention methods, and other information necessary to protect, detect, report, and respond to computer security incidents.

Product Evaluation or Certification

For this service, the CSIRT may conduct product evaluations on tools, applications, or other services to ensure the security of the products and their conformance to acceptable CSIRT or organizational security practices. Tools and applications reviewed can be open source or commercial products. This service can be provided as an evaluation or through a certification program, depending on the standards that are applied by the organization or by the CSIRT.

Summary

This document outlines and defines various incident handling services and several other services that can be provided by a CSIRT. Some teams may offer many services from this list; others may only be able to provide a few; still other teams may share the responsibility for providing these services with other parts of their parent or host organization, or they may outsource some services to an incident response or managed security services provider. As mentioned at the beginning of this document, to be considered a CSIRT, a team must provide one or more of the incident handling services: incident analysis, incident response on site, incident response support, or incident response coordination.

Experience has shown that whatever services a CSIRT chooses to offer, the parent organization or management must ensure that the team has the necessary resources (people, technical expertise, equipment, and infrastructure) to provide a valued service to their constituents, or the CSIRT will not be successful and their constituents will not report incidents to them.⁸

In addition, as changes occur in technology and Internet use, other services may emerge that need to be provided by CSIRTs. This list of services will therefore need to evolve and change over time.

If you have any comments on this list of CSIRT services or have suggestions for services that you think should be added, we would like to hear from you. Please send email to csirt-info@cert.org.

References

- [1] West-Brown, Moira J.; Stikvoort, Don; & Kossakowski, Klaus-Peter. *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-98-HB-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1998.
<http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html>.
- [2] Kossakowski, Klaus-Peter. *Information Technology Incident Response Capabilities*. Hamburg: Books on Demand, 2001 (ISBN: 3-8311-0059-4).

⁸ If the CSIRT does not provide the services but outsources the activities to another organization such as a managed security services provider, it must still ensure that the same standards for staffing, equipment, and infrastructure are adhered to, in order to protect the CSIRT and organizational data and services.

- [3] Kossakowski; Klaus-Peter & Stikvoort, Don. "A Trusted CSIRT Introducer in Europe." Amersfoort, Netherlands: M&I/Stelvio, February, 2000.
<http://www.ti.terena.nl/process/ti-v2.pdf> (see "Appendix E, Basic Set of Information").