WHAT SKILLS ARE NEEDED WHEN STAFFING YOUR CSIRT?

If you want to build a computer security incident response team (CSIRT) with capable incident handlers, you need people with a certain set of skills and technical expertise, and with abilities that enable them to respond to incidents, perform analysis tasks, and communicate effectively with your constituency and other external contacts. They must also be competent problem solvers, must easily adapt to change, and must be effective in their daily activities. It is not often easy to find such qualified staff, so sometimes CSIRTs nurture and train internal staff members to advance into these incident handling roles.

In this document, we describe a minimum set of basic skills that CSIRT staff members should have. This skill summary is based on the early incident handling experiences of the CERT Coordination Center (CERT/CC), our observations of CSIRTs, and the experiences others in the community have shared with us over the years. We also suggest some of the additional "specialist" skills that a few members of the team should have (or have access to)—experts who can be called upon for technical help or guidance when a special need arises. However, these special skills are not our main focus, which is to highlight the basic skills for incident handling staff.

The composition of CSIRT staff varies from team to team and depends on a number of factors, such as

- mission and goals of the CSIRT
- nature and range of services offered
- available staff expertise
- constituency size and technology base
- anticipated incident load
- severity or complexity of incident reports
- funding

Many teams possess a core group of individuals who provide the basic level of incident handling services.[1] Each CSIRT staff member is expected to have some minimum set of basic skills to do the work and be effective in their work responsibilities.

While it's expected that any team member should be able to identify whether an intruder tool found in an incident is one previously known to the response team, only a subset of that staff may have the skills to analyze intruder-developed exploit tools, identify and document the impact of resulting attacks, and provide insight to the rest of the team members. Thus, it is also important for the CSIRT to include or have access to other experts with an in-depth understanding of the technologies that the team and the constituency use. These experts, who might be in another part of the organization, can provide technical guidance or advice; they might also provide training and mentoring to other team members. This additional level of expertise is a resource that can help to broaden and deepen the technical knowledge and capabilities of the team.

Distribution Statement A: Approved for Public Release; Distribution Is Unlimited

If a CSIRT is unable to find internal experts or to hire or train staff to provide the necessary specialist skills, they may be able to develop relationships with experts in the field to provide the necessary skills. These types of creative relationships, of course, require advance negotiation and/or trusted relationships between the CSIRT and the expert(s). These relationships can be defined in formal or informal agreements (with clearly defined requirements or expectations) that outline how the request for assistance is made, and what restrictions are placed on information that is shared. When a situation arises where in-house knowledge is not enough, these technical specialists can be called upon to fill the gap in expertise.

When more complex incidents are reported, CSIRTs will need to supplement or expand their basic skills to include more in-depth knowledge so that staff members can understand, analyze, and identify effective responses to reported incidents.

Basic Skills

The set of basic skills we believe CSIRT staff members need to have are described below, separated into two broad groups: ***personal skills*** and ***technical skills***.

We haven't implied any order of priority in the listing that follows. And, as the internet technologies and usage evolve, this set of basic skills will also need to evolve.

Financial plans and budgets should include funds for sustaining the overall quality of the CSIRT. To enable CSIRT staff to keep pace with the changes in technology and usage, there should be an ongoing budgeting plan for continuing education or refresher courses so CSIRT staff can continue to be effective incident handlers. In addition, where appropriate, budget plans should also include funds to provide opportunities for professional development to further enhance the team members' knowledge and abilities, keep them engaged and energized about CSIRT work, and (at the same time) expand the overall capabilities of the team.

1. Personal Skills

It is important for CSIRT staff to have a wide range of personal skills because a major part of the incident handler's daily activity will involve communicating with their constituency, their own team members, other response teams, a variety of technical experts, and other individuals who may have various levels of technical understanding. The reputation of a CSIRT can be made or lost by the professional interactions of its team members.

Many of the skills outlined below contribute to the overall success of the CSIRT in its daily interactions. For example, CSIRT staff who are technically competent and have excellent communication skills can solidify the reputation of the team and strengthen the respect with which a team is held (both by the constituency and by others with whom the team interacts). They can also be a role model for other team members. On the other hand, the interactions of a team member who is a technical expert, but who possesses poor communication skills can result in miscommunications that can severely damage a team's reputation and standing in the community, especially when those communications are misinterpreted or mishandled.

1.1. Communication

The ability to communicate effectively is a critical component of the skills needed by CSIRT staff. They need to be effective communicators to ensure that they obtain and supply the information necessary to be helpful. They need to be good listeners, understanding what is said (or *not* said) to enable them to gain details about an incident that is being reported. CSIRT staff must also remain in control of these communications to most effectively determine what is happening, what facts are important, and what assistance is necessary. They need to be able to adapt to the appropriate level of discussion without being condescending or talking above the comprehension level of the listener (whether the listener is a user, administrator, manager, or another person in the community).

Written Communication

For many CSIRTs, a large part of its communication occurs through the written word. This communication can take many forms, including

- responses in email concerning incidents
- documentation of event or incident reports, vulnerabilities, and other technical information
- notifications and/or guidelines that are provided to the constituency
- internal development of CSIRT policies and procedures
- other external communications to staff, management, or other relevant parties

CSIRT staff members must be able to write clearly and concisely, describe activities accurately, and provide information that is easy for their readers to understand.

Oral Communication

The ability to communicate effectively though spoken communication is also an important skill to ensure that CSIRT staff members can say the right words to the right people. Oral communication often occurs through telephone exchanges or face-to-face discussions and can involve a variety of individuals, for example

- CSIRT team members
- system and network administrators (or other IT staff)
- application owners/developers

- members of other response teams
- constituents or users (of the systems)
- subject matter or technical experts
- security officers
- management or other administrative staff
- human resources staff
- law enforcement or legal staff
- press/media/public relations staff
- vendors

In some cases, selected members of the team may be primary contacts with the above groups and/or serve the role of "official spokesperson" for the CSIRT, presenting the mission and goals of the CSIRT, and speaking authoritatively about the services and activities undertaken by the team.

Whether by telephone, in person, or through printed materials, the method of communication, the language, and the tone of voice should remain professional, calm, and confident.

1.2. Presentation Skills

Although all CSIRT incident handling staff may interact daily with members of the constituency, they may not all be comfortable in front of a large audience or an audience of their peers. Moreover, staff may find themselves facing difficult, controversial, or potentially hostile situations that must be handled in a professional way; they need to be adept at effectively responding without harming the reputation of the CSIRT or offending others. Gaining confidence in presentation skills will take time and effort for staff members to become more experienced and comfortable in these situations.

Within the context of "specialist" skills, the CSIRT often needs one or several staff members with strong presentation skills. Their skills might be needed for a technical presentation, management or sponsor briefings, a panel discussion at a conference, or some other form of public-speaking engagement. The specialist's skills might extend, for example, to providing expert testimony in legal or other proceedings on behalf of the CSIRT or a constituent member. These knowledgeable staff members represent the CSIRT and often will need to explain its mission and goals, services, strategic direction, etc. Such staff also understand that any hostility they encounter may be the result of frustration with a specific issue that is being debated, the team's policies and procedures, the organization, or even another party that might be associated with the CSIRT in some way. They understand the need to remain calm, keep the issues in perspective, appropriately represent the CSIRT and/or constituency being served, and not take hostile questions and interactions personally.

1.3. Diplomacy

CSIRT staff members often find that the community with whom they interact may have a variety of goals and needs. This community may have varying levels of knowledge and degrees of excitement; some people may feel overwhelmed with the gravity of their situation; they may be anxious, frustrated, or angry. Still others may be aggressive or try to "trick" the CSIRT staff member into providing inappropriate information. Skilled CSIRT staff will be able to anticipate potential points of contention, be able to respond appropriately, maintain good relations, and avoid offending others. They also will understand that they are representing the CSIRT and/or their organization. Diplomacy and tact are essential.

1.4. Ability to Follow Policies and Procedures

Another important skill that CSIRT staff members need is the ability to follow and support the established policies and procedures of the organization or team. From a historical perspective, CSIRT staff should understand how and why the policies and procedures came into existence. To ensure a consistent and reliable incident response service, CSIRT staff must be prepared to accept and follow the rules and guidelines, even if these are not fully documented and regardless of whether the staff member personally agrees with them. On the other hand, if the staff feel strongly that change is required and if they want to approach management with suggested changes, they should be permitted to propose changes. They should articulate why the change(s) will improve CSIRT operations and the constituency being served.

1.5. Team Skills

CSIRT staff must be able to work in a team environment as productive and cordial team players. CSIRT staff need to be aware of their responsibilities, contribute to the goals of the team, and work together to share information, workload, and experiences. They must be flexible and willing to adapt to change. They also need team skills for interacting with other parties (for example, members of other incident response teams and other members of the organization, such as IT staff, site security officers, and network operators). If a CSIRT staff member isn't willing to cooperate and support the rest of the CSIRT staff, team morale will be affected, and there could be resentment among other members of the team. This resentment could result in a loss of team productivity, effectiveness, reputation, or potential loss of other CSIRT staff members (who leave because they are dissatisfied with the work environment).

As the CSIRT evolves and grows, there may be a need for one or more team members who can act in a leadership role to support the smaller groups or technical teams within the CSIRT. These leaders manage the day-to-day activities of the staff on the smaller team and also work with the CSIRT manager on decisions relating to strategic direction, CSIRT policy, infrastructure, and/or operational actions that require more than a technical background to identify the best approach.

This is another place where specialist skills come into play. However, an effective combination of technical ability and management/leadership skills is not easy to find. An individual can gain these skills over time, and some individuals may evolve into a leadership role as they gain experience and training. But it's important to recognize that technical leadership is not a skill that is suddenly available on demand after an individual has taken a leadership training class. Rather, it is something the team needs time to nurture and develop, or seek outside the CSIRT. Management may need to budget and/or recruit for leadership positions (whether staff is selected from within or outside of the CSIRT).

1.6. Integrity

The nature of CSIRT work means that the team members often deal with information that is sensitive[2] and, occasionally, they might have access to information that is newsworthy. CSIRT staff must be trustworthy, discrete, and able to handle information in confidence according to the CSIRT guidelines, any constituency agreements or regulations, and/or any organizational policies and procedures.

In their efforts to provide technical explanations or response, CSIRT staff must be careful to provide appropriate and accurate information while avoiding the dissemination of any confidential information that could detrimentally affect another organization's reputation, result in the loss of the CSIRT's integrity, or affect other activities that involve other parties.

Thus, it is important that the team members understand the distinction between their "customer service" role in providing assistance to their constituency and the need to ensure that information is protected and handled appropriately. CSIRT staff may find themselves in a position where they know about information and could comment on a topic, but doing so could acknowledge or disclose information that was provided in confidence or that could affect an ongoing investigation. CSIRT staff must remain aware of their responsibilities and not be caught "off guard" and make unauthorized disclosures.

1.7. Knowing One's Limits

Another important ability that CSIRT staff must have is to be able to readily admit when they have reached the limit of their own knowledge or expertise in a given area. However difficult it is to admit a limitation, individuals *must* recognize their limitations and actively seek support from their team members, other experts, or their management. Otherwise, the reputation of a team can be severely affected by a CSIRT staff member who has provided incorrect information or guidance to others.

1.8. Coping with Stress

CSIRT staff often find themselves in stressful situations. They need to be able to recognize when they are becoming stressed, be willing to make their fellow team members aware of the situation, and take (or seek help with) the necessary steps to control and maintain their composure. In particular, they need the ability to remain calm in tense situations—ranging from an excessive workload to an aggressive caller to an incident where human life or a critical infrastructure may be at risk. The team's reputation, and the individual's personal reputation, will be enhanced or will suffer depending on how such situations are handled.

1.9. Problem Solving

CSIRT staff are confronted with data every day, and sometimes the volume of information is large. It is essential that staff be able to

- determine the relevance of the data provided
- identify what information is important, missing, or might be misleading or incorrect
  - decide on how to handle that data

Without good problem-solving skills, staff members could become overwhelmed with the volumes of data related to incidents and other tasks that need to be handled. Problem-solving skills also include an ability for the CSIRT staff member to "think outside the box" or look at issues from multiple perspectives to identify relevant information or data. This includes, for example,

- knowing who else in the team they might contact or approach for additional information, creative ideas, or added technical insight
- recognizing and seeking additional information from other resources (e.g., literature searches, past incidents that may involve similar activities, similarities in attack techniques or tools, other sources of information)
- verifying information through alternative approaches
- synthesizing information to determine relationships or to correlate with other incident data

1.10. Time Management

Along with problem-solving skills, it is also important for CSIRT staff to be able to manage their time effectively. They will be confronted with a multitude of tasks ranging from analyzing, coordinating, and responding to incidents, to performing duties such as prioritizing their workload, attending and/or preparing for meetings, completing time sheets, collecting statistics, conducting research, giving briefings and presentations, traveling to conferences, and possibly providing onsite technical support.

Sometimes, even when they are given criteria for prioritizing tasks, staff may find it difficult to appropriately prioritize and manage the myriad responsibilities that they are assigned in accordance with those criteria. To stay productive, CSIRT staff must be able to balance their effort between completing the tasks assigned to them, recognizing when to seek help or guidance from their management (when workload is becoming overwhelming), and avoiding a state where constant re-prioritizing as new tasks arise prevents them from actually completing their tasks!

The skills outlined in the previous sections focused on team members' personal and organizational skills. Another important component of the baseline skills needed for a CSIRT to be effective is the technical skills of the staff. These skills, which define the depth and breadth of understanding of the technologies used by the team and the constituency it serves, are outlined in the sections below.

2. Technical Skills

The basic technical skills that CSIRT staff need have been separated into two categories: ***technical foundation*** skills and ***incident handling*** skills.

Technical foundation skills require a basic understanding of the underlying technologies used by the CSIRT and the constituency, as well as an understanding of issues that affect that team or constituency. Such issues may include

- the type of incident activity that is being reported or seen by the community
- the way in which CSIRT services are being provided (the level and depth of technical assistance provided to the constituency)
- the responses that are appropriate for the team (e.g., what policies and procedures or other regulations must be considered or followed while undertaking the response)
- the level of authority the CSIRT has in taking any specific actions when applying technical solutions to an incident reported to the CSIRT

Incident handling skills require an understanding of the techniques, decision points, and supporting tools (software or applications) required in the daily performance of CSIRT activities.

In a few of the sections included below, we refer to "specialist" skills. These specialists have a broader depth of understanding of the technology: host or system security issues, application-level expertise, extensive skills and knowledge of the tools used to examine the security of systems and networks, extensive skills in software engineering and development, programming or scripting languages, forensics expertise, or sophisticated management skills. These individuals are the added-value resource the CSIRT calls upon. They may be the more senior members of the team, adjunct members the team, other staff from within the organization, or external trusted experts.[3] They bring to the team expertise in technical issues and strategic leadership into the research, examination, and analysis of computer security topics and trends.

2.1. Technical Skills

In the broader view of CSIRT activities, the technical foundation skills and knowledge are important skills that are used in the daily operations and team interactions with the constituency. These baseline skills are needed to understand how systems and software are configured and how they work, the risks associated with the various technologies in use, and the strategies and approaches[4] to protecting, securing, and/or repairing the systems.

The concepts associated with these baseline skills are similar; regardless of the underlying software and hardware that is used to perform the work (e.g., the principles will be the same). Building upon such a baseline, then, are the more specialized skills and knowledge needed for any tools and technologies (software, hardware, policy) in use by the team or constituency. Examples of some of these basic technical foundation skills are listed in the following sections.

2.1.1. Security Principles

CSIRT staff members need to have a general understanding of basic security principles such as

- confidentiality
- availability
- authentication
- integrity

- access control
- privacy
- non-repudiation

Knowledge about security principles are necessary for the CSIRT staff to understand potential problems that can arise if appropriate security measures have not been implemented correctly, as well as the potential impacts to the constituents' systems or, for that matter, the CSIRT's systems. CSIRT staff with this understanding will be better prepared to determine their constituents' needs in securely configuring systems to prevent misuse or compromises and also be better prepared to provide appropriate technical assistance and guidance when breaches do occur.

2.1.2. Security Vulnerabilities/Weaknesses

To understand how any specific attack is manifested in a given software or hardware technology, the CSIRT staff need to be able to first understand the fundamental causes of vulnerabilities through which most attacks are exploited. They need to be able to recognize and categorize the most common types of vulnerabilities and associated attacks, such as those that might involve

- physical security issues
- protocol design flaws (e.g., man-in-the-middle attacks, spoofing)
- malicious code (e.g., viruses, worms, Trojan horses)
- implementation flaws (e.g., buffer overflow, timing windows/race conditions)
- configuration weaknesses
- user errors or indifference

2.1.3. The Internet

It is important that CSIRT staff also understand the internet. Without this fundamental background information, they will struggle or fail to understand other technical issues, such as the lack of security in underlying protocols and services used on the Internet or to anticipate the threats that might occur in the future.

At a minimum, CSIRT staff members should know about the history, philosophy, and structure of the internet, and the infrastructures that support it.

2.1.4. Risks

CSIRT staff members need to have a basic understanding of computer security risk analysis. They should understand the effects on their constituency of various types of risks (such as potentially widespread Internet attacks, national security issues as they relate to their team and constituency, physical threats, financial threats, loss of business, reputation, or customer confidence, and damage or loss of data). Newly hired CSIRT staff may not have this knowledge and will need guidance and mentoring to ensure they understand the risks that may affect the constituency being served, as well as any risks that might affect the CSIRT itself.

2.1.5. Network Protocols

Members of the CSIRT staff need to have a basic understanding of the common (or core) network protocols that are used by the team and the constituency they serve. For each protocol, they should have a basic understanding of the protocol, its specification, and how it is used. In addition, they should understand the common types of threats or attacks against the protocol, as well as strategies to mitigate or eliminate such attacks.

For example, at a minimum, staff should be familiar with protocols such as IP, TCP, UDP, ICMP, ARP, and RARP. They should understand how these protocols work, what they are used for, the differences between them, some of the common weaknesses, etc. In addition, staff should have a similar understanding of protocols such as TFTP, FTP, HTTP, HTTPS, SNMP, SMTP, and any other protocols that are used by the CSIRT or its constituency.

The specialist skills include a more in-depth understanding of security concepts and principles in all the above areas in addition to expert knowledge in the mechanisms and technologies that lead to flaws in these protocols, the weaknesses that can be exploited (and why), the types of exploitation methods that would likely be used, and strategies for mitigating or eliminating these potential problems. They would have expert understanding of additional protocols or internet technologies (DNSSEC, IPv6, IPSEC, other telecommunication standards that might be implemented or interface with their constituent's networks, such as ATM, BGP, broadband, voice over IP, wireless technology, other routing protocols, or new emerging technologies, etc.) and provide expert technical guidance to other members of the team or constituency.

2.1.6. Network Applications and Services

CSIRT staff members need a basic understanding of the common network applications and services that the team and the constituency use (DNS, NFS, SSH, etc.).[5] For each application or service, they should understand the purpose of the application or service, how it works, its common usages, secure configurations, and the common types of threats or attacks against the application or service, as well as mitigation strategies.

The specialist skills include expanded technical insight into these applications and services, as well as new emerging products that may be integrated into the CSIRT constituency. The specialist could also provide insight into issues and security considerations that need to be discussed, addressed, or resolved in implementing any existing or new systems, new applications, or network architecture designs. At the specialist level, understanding also includes experience in other, less frequently used applications or more obscure services that might be used by, or of interest to, the CSIRT or constituency (for example, a new implementation of wireless services or introduction of a public key infrastructure into the constituency's environment).

2.1.7. Network Security Issues

CSIRT staff members should have a basic understanding of the concepts of network security and be able to recognize vulnerable points in network configurations. They should understand the concepts and basic perimeter security of network firewalls (design, packet filtering, proxy systems, DMZ, bastion hosts, etc.), router security, potential for information disclosure of data traveling across the network (e.g., packet monitoring or "sniffers"), or threats relating to accepting untrustworthy information.

The specialist would have the ability to anticipate, identify, isolate, and describe potential new vulnerabilities that could affect the constituency (or CSIRT itself) as a result of changes in network design, hardware, or software. They would be able to identify and develop tools or processes that would mitigate or resolve these potential security weaknesses.

2.1.8. Host/System Security Issues

In addition to understanding security issues at a network level, CSIRT staff need to understand security issues at a host level for the various types of operating systems (UNIX, Windows, or any other operating systems used by the team or constituency). Before understanding the security aspects, the CSIRT staff member must first have

- experience using the operating system (user security issues)
- some familiarity with managing and maintaining the operating system (as an administrator)

Then, for each operating system, the CSIRT staff member needs to know how to

- configure (harden) the system securely6
- review configuration files for security weaknesses
- identify common attack methods
- determine if a compromise attempt occurred
- determine if an attempted system compromise was successful
- review log files for anomalies
- analyze the results of attacks
- manage system privileges
- secure network daemons
- recover from a compromise

2.1.9. Malicious Code (Viruses, Worms, Trojan Horse programs)

CSIRT staff must understand the different types of malicious code attacks that occur and how these can affect their constituency (system compromises, denial of service, loss of data integrity, etc.). Malicious code can have different types of payloads that can cause a denial of service attack or web defacement, or the code can contain more "dynamic" payloads that can be configured to result in multifaceted attack vectors. Staff should understand not only how malicious code is propagated through some of the obvious methods (disks, email, programs, etc.) but also how it can propagate through other means such as PostScript, Word macros, MIME, peer-to-peer file sharing, or boot-sector viruses that affect operating systems running on PC and Macintosh platforms. CSIRT staff must be aware of how such attacks occur and are propagated, the risks and damage associated with such attacks, prevention and mitigation strategies, detection and removal processes, and recovery techniques.

Specialist skills include expertise in performing analysis, black box testing, or reverse engineering on malicious code that is associated with such attacks and in providing advice to the team on the best approaches for effective response.

2.1.10. Programming Skills

Some team members need to have system and network programming experience. The team should ensure that a range of programming languages is covered on the operating systems that the team and the constituency use. For example, the team should have experience in

- C
- Perl
- Awk
- Java
- shell (all variations)
- other scripting tools

These scripts or programming tools can be used to assist in the analysis and handling of incident information (e.g., writing different scripts for counting and sorting through various logs, searching databases, looking up information, extracting information from logs/files, collecting and merging data).

Additionally, CSIRT staff should understand the concepts of and techniques for secure programming. They need to be aware of how vulnerabilities can be introduced into code (e.g., through poor programming and design practices) and how to avoid these in any tools or products that they may develop for the team or their constituency.

The specialist should have expert skills in software development and programming in multiple languages. They would also bring to the team skills in software engineering concepts. Their expertise could also extend to providing technical leadership and mentoring or guidance to other members of the team.

2.2. Incident Handling Skills

Within the broad range of technical skills needed to undertake incident handling is a subset of skills the CSIRT staff also need. We call these "incident handling" skills, and they are associated with the underlying daily operational activities of the CSIRT. It is worth noting that while these underlying concepts relating to incident handling skills can be similar across many different CSIRTs, the specific implementation, policies, and procedures for how these concepts are applied will be very specific within each team (and based on other factors mentioned previously in the Introduction).

2.2.1. Local Team Policies and Procedures

The CSIRT incident handlers must be trained in the local policies and procedures that govern the operation of their team. Every aspect of the work will most likely lead back to a policy or procedure that must be followed or to other directives from management. CSIRT staff need this background information and must have a firm grasp of the guiding principles; otherwise, they won't understand the framework and boundaries in which they apply their range of skills and knowledge. Every CSIRT staff member must be able to support these policies and procedures, not only at the team level but also at an organizational level (or even any that are associated with the constituency they serve as it applies to their relationship with that constituency).

2.2.2. Understanding/Identifying Intruder Techniques

Building on their technical foundation skills (covered in Section 2.1), all CSIRT incident handlers must be able to recognize known intrusion techniques based on the footprints or artifacts[7] left by different types of attack in the incident reports they handle. In addition, they need to know the appropriate methods to protect against these known attack techniques and the risks associated with the attacks.

Given real incident data, the incident handler should be able to use the knowledge that they have gathered from any existing documented analyses to identify the types of attack and recognize specific intruder tools or toolkits, techniques used, or other malicious code. With each type of attack, they should understand the associated risks and effects, the relative severity, and the mitigation, prevention, or recovery methods.

Another important incident handling skill is the analysis of and correlation between incidents to notice what has *not* been seen before (a new attack technique, footprint, intruder tool, attack vector). Being able to identify such abnormal (or unexpected) activity might lead to the recognition of new attacks or potential vulnerabilities that warrant further investigation or analysis (which might be undertaken by more senior members of the team or other experts). Some team members will require additional specialist skills and knowledge to be able to

- identify a new vulnerability
- undertake technical analysis of intruder tools and techniques
- recognize new intrusion techniques based on the footprints and their effects
- document analyses of artifacts as reference material for other team members (this work might also extend to providing guidance to help other CSIRT staff identify footprints, associated risks, and prevention methods)

2.2.3. Communicating with Sites

Much of the communication undertaken by CSIRT incident handlers is conducted online, commonly through email. The correspondence often requires the transmittal of incident data in a secure manner. As a result, it is crucial that CSIRT staff be fully conversant in the use of email and MIME functionality, as well as tools and methods to identify contact information for other sites—including understanding which points of contact are most appropriate—and the appropriate encryption technologies to be used.

They should also understand the functionality and use of various tools to facilitate the review and interpretation of incident data (compressed file formats and tools, archiving tools such as UNIX tar or WinZIP, uuencode/decode, etc.). In addition, it is important to ensure that the incident handling staff are cognizant of the types of coordination that occur in interactions between and across these other teams (the amount of information that is to be shared and how that information sharing is to be achieved while adhering to their own team's information disclosure policies and procedures).

2.2.4. Incident Analysis

It has been said by others in the community that CSIRT incident handlers are like detectives. When they analyze an incident report, they are looking to determine answers to questions such as [8]

- Who is involved?
- What has happened?
- Where did the attack originate from?
- When (what time frame)?
- Why did it happen?
- How was the system vulnerable or how did the attack occur?
- What was the reason for the attack?

They also want to identify what critical information is missing, where clarification is required, and the effect and scope of the activity. They should be able, where possible, to determine the tools or attacks used, the level of access gained, time frames, damage or implications associated with the attack, and the hosts/sites involved.

CSIRT staff also need to know their responsibilities with regard to the level and depth of analysis to be performed, along with any guidelines relating to the appropriate collection of data (from their own operational policies and/or any actions they take that could potentially affect future evidentiary use or legal investigations).

CSIRT staff must be able to recognize the importance of the activity in relation to the team's priorities, as well as determine the appropriate response. Further, they need to analyze new incident activity reports to determine whether these reports may relate in some way to other existing reports (related timings of attacks, attack signatures, specific vulnerabilities being exploited, etc.) and to identify any trends or similar types of activities that may affect their constituency.

Specialist skills in the area of incident analysis might involve in-depth analysis of tools, scripts, and other artifacts that are discovered during the course of handling an incident and that the other CSIRT staff are not able to identify. This analysis could also include forensic analysis or data collection for use in criminal investigations. This expert assistance might be requested to reverse engineer exploits and/or to undertake code reviews.[9]

2.2.5. Maintenance of Incident Records

Another major role of the incident handler is to maintain incident records. While this is not necessarily a "skill" in the same sense as other skills discussed in this section, it is an important process that should be integrated into the CSIRT operations and followed by all team members who are responsible for incident handling functions.

To ensure that incident records are well maintained, every CSIRT incident handler must understand the technology used to maintain the incident report records, supporting information, and any other associated files. It is also very important that incident records are well documented, consistently maintained, and current. Doing so will give a clear picture of the current state of activity and what work remains. Keeping good records also facilitates smooth transitions between team members should the need arise to "hand off" a report to another member of the team.

Summary

CSIRT staff must have a set of basic personal and technical skills. Many of the skills needed by CSIRTS are adapted from the areas of traditional system and network administration and project management. Whether the CSIRT staff are nurtured and "grown" from internal organizational staff or recruited and hired as additions to the existing team, it is important that they have the baseline skills.

Providing an environment in which the staff can use their skills and develop further technically and professionally will improve the CSIRT's ability to provide valued service to the constituency they serve, as well as enable the team to support the new technologies that are integrated into the CSIRT and the constituency.

This discussion of the list of skills is not comprehensive. While we have referred to example protocols, services, or other skills and expertise, we haven't included everything that a team might be required to know about for their particular CSIRT environment or constituency.

Just as CSIRTs evolve and need to adapt to change, we expect that over time, documents such as this one will need to be revised as the "bar" is raised. If you would like to comment on other basic skills that CSIRT staff should have or that you believe are missing from this list, we'd like to hear from you. Please contact us.

Notes

[1] See the Handbook for CSIRTs, pages 23-35, or the "CSIRT Services" document.

[2] Depending on the environment, they may have access to classified information as well.

[3] They may also be individuals with whom a more formalized agreement has been made (non-disclosure agreements, service-level agreements, negotiated support for other technical advice or guidance, etc.).

[4] Some coordinating CSIRTs may only provide the guidance or suggestions to others that will undertake the work; however, the CSIRT staff still need to have the skills in order to provide the appropriate information.

[5] This could also extend to having knowledge about other programs, or protocols that have been used in the past or that might also be available in some parts of a constituency (Telnet, rlogin, rsh, rcp, etc.).

[6] A collection of security improvement modules that can be used to configure a system securely is available from *The CERT Guide to System and Network Security Practices*, Julia H. Allen, Addison-Wesley, 2001.

[7] We define artifacts as remnants that are found on a host that has been compromised. These could include scripts, archives, toolkits, malicious code, binary files, logs, Trojan horse programs, or other software used to break into a system.

[8] Teams may or may not focus on finding the answers to all of these questions. The CERT/CC, for example, focuses on the *what* and *how*, not the *who* and *why*. They want to determine what has occurred and, from a technical or security perspective, how it happened. While they may discover who caused an attack and the motivation for the attack, it is not a primary goal of the analysis. Other CSIRTs, depending on their roles and responsibilities, may need to pursue the answers to these questions to support investigative actions.

[9] It should be noted, however, that not all teams will have a requirement for this set of skills and the team may depend on other organizations to perform the analyses.

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org

Copyright 2017 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

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.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use:* 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 external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

CERT® is a registered mark of Carnegie Mellon University.

DM-0004386