


Module 3

CSIRT Operation

[Presenter Name]

[Date]



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Agenda

By the end of this module, you will be able to:

- Describe the incident management process
- Step through relevant tools, references, and technologies
- Identify causes of incidents
- Clarify how to respond to attacks
- Define best practices for publishing security bulletins and other communications
- Describe how to handle media issues
- Demonstrate how to test, verify, and improve incident management processes
- Practice responding to an incident

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Section 1:

Incident Management Processes

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Recognize Signs of Attacks

- Time matters!
- Discuss
 - Document
 - Practice
 - Use simulators and emulators
 - Review incident list of previous threats
 - Consider numerous threats



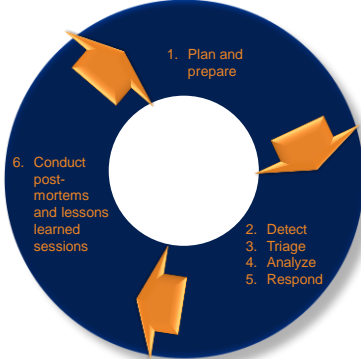
Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Incident Management Processes

1. Plan and prepare
2. Detect
3. Triage
4. Analyze
5. Respond
6. Conduct post-mortems and lessons learned sessions

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Incident Management Processes



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

1. Plan and Prepare

- Maintain contact information up-to-date
- Recognize signs of attacks
- Maintain and update policies



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Maintain Internal Contact Information

- Executive leadership
 - Business managers
 - IT representatives
- Legal department representatives
 - Human Resources representatives
 - Public Relations representatives
- Other security groups, including physical security
 - Audit and risk management specialists
 - Law enforcement liaisons or investigators

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Maintain External Contact Information

- Contracted external support personnel
 - Security organizations such as other CSIRTs, CERTs
 - Managed service providers
 - Business partners
- Law enforcement organizations
 - Emergency authorities
 - Appropriate government organizations
- Customers
 - General public

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Value of Conferences

- Build relationships
- Meet people face-to-face
- Learn new skills
- Increase visibility of your organization
- FIRST.Org, Black Hat, CanSecWest, Hack In The Box



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Worldwide Teams and Organizations

- www.first.org
- www.apcert.org
- oic-cert.org/en/index.html
- www.africacert.org/home/
- www.terena.nl/activities/tf-csirt/
- www.infragard.net
- www.isaccouncil.org
- puck.nether.net/mailman/listinfo/nsp-security



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Learning Check

How would a CSIRT establish internal relationships differently than external relationships?



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

2. Detect

- Controls and procedures should be in place to manage security incidents
- Not all information security events indicate an attack
 - Accidental
 - Technical
 - Non-technical
- Ensure that incidents are documented
- Share relevant information



Training Module 3, CSIRT Operation, Version 2. © 2016 FIRST

2. Detect

- Key Steps:
- Monitor and log system and network activity
 - Discover and communicate
 - Collect symptoms and information
 - Collect situational awareness information—internal and external
 - Log activities, results, and decisions for later analysis
 - Gather and store digital evidence
 - Update needed changes to documentation



Training Module 3, CSIRT Operation, Version 2. © 2016 FIRST

3. Triage



- Address the most potentially damaging impacts to the organization
- Severity of the incident determines priority
 - Before you react, check the information available
 - Have a list of standard questions to begin the process of evaluating the situation:
When did the problem start? What triggered it? What are the short-term and long-term business impacts?
 - Work quickly and efficiently
 - Take good notes

Training Module 3, CSIRT Operation, Version 2. © 2016 FIRST

4. Analyze

Incident Analysis: Assess the severity and determine the urgency

- Identify the possible causes
- Translate the symptoms into potential causes
- Do not announce a threat or leak
- Do not make assumptions based on the incident reporter's information
- Evaluate the situation and verify your data



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Malware Analysis

- Malware: executable content with unknown functionality that is resident on a system
- Make sure that you know why you are running tests for malware
- Don't use your computer to test for malware! Don't test for malware on a live network in your organization!
- Two types of analysis:
 - Static analysis: Analyzing code that is **not** running at the time of analysis
 - Dynamic analysis: Analyzing code that **is** running at the time of analysis



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Digital Media Analysis

- Forensic analysis of a system based on a cycle of data gathering and processing the information gathered
- The more accurate and complete the data, the better and more comprehensive the evaluation can be
- Isolate the computer or network on which a threat has been detected
- Focus on data from systems that aren't running and perform your analysis on a copy of the data
- Capture information in accordance with its expected lifespan
- Remember that the vast majority of files have not been used at all in the last year and deleted file information can survive intact for months or years



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Digital Media Analysis

- **Option 1:** Capture volatile information about processes and network connections, file attributes, configuration files, logfiles, and assorted other files
- **Option 2:** Halt the machine, remove the disks, and make copies of the data for forensic analysis
- How to proceed?
 - Copy individual files
 - Make a backup
 - Copy individual disk partitions
 - Copy the entire disk



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Network Traffic Analysis



- Network traffic analysis focuses on traffic performance
- NetFlow and IPFIX help collect this information

- Incident analysis looks deeper into communication: Wireshark, tcpdump, and Splunk for wired and wireless media
- Wireless can be used to locate unauthorized stations; can use Wi-Fi or GSM
- Two modes of capture: session data and full data capture

Image source: AMS-IX (Amsterdam Internet Exchange)
Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Learning Check

What are some business impacts related to an incident?



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

5. Respond

- Contact the local CSIRT, or a local correspondent whose position is related to security
- Resources:
<http://www.first.org/members/map/>
<https://www.trusted-introducer.org/>
- Standard security email addresses
- Standard security web page
- whois and domain name



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Disseminate Information



- The level at which information is disseminated depends on the severity and scope of the attack or vulnerability
- Notification can provide an authoritative answer, stop users from guessing at the impact of the vulnerability, and prevent them from opening support cases
- CVSS provides a standardized method for rating IT vulnerabilities and determining the urgency of response

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

6. Conduct Post-Mortem and Lessons Learned Sessions

- After an incident occurs, take time to conduct a post-mortem session on history, prevention, and impacts
- Use the “five whys” to get to a root cause
- Can result in new or changed:
 - Requirements for information security controls
 - Threat and vulnerability information
 - Information security incident management plan
- Share the post-mortem with the entire CSIRT and at a high level outside of the CSIRT



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Learning Check

How do you conduct a post-mortem session?



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Questions?

What questions do you have about this lesson?



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

**Section 2:
Tools and Technologies**

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Tools

- Different categories of tools can be useful:
 - Text manipulation: extracts and sorts information
 - Automation: repetitive tasks
 - Databases: collect and store large amounts of data
- Information received in different formats must be processed for existing tools
- CSIRT team must automate its processes



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Tools

- Network auditing tools
 - AbuseHelper
 - Wireshark
- Network intrusion detection tools
 - Snort
- Forensics tools
 - Sleuth Kit
 - EnCase
- Network analysis
 - whois
 - Splunk
 - dig
- Encryption
 - GnuPG



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Tools

- Incident-tracking tools
 - RTIR
- Command-line tools
 - sed
 - AWK
 - grep
- Scripting languages
 - Python
 - Perl
- Databases
 - SQLite
 - MySQL
 - PostgreSQL



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Tools

European Union Agency for Network and Information Security (ENISA)
<http://www.enisa.europa.eu/activities/cert/support/chiht>



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Technologies: Need for Automation

- Security incidents increasing
- So is the volume of information that needs to be examined or shared
- More CSIRT operations need to be automated



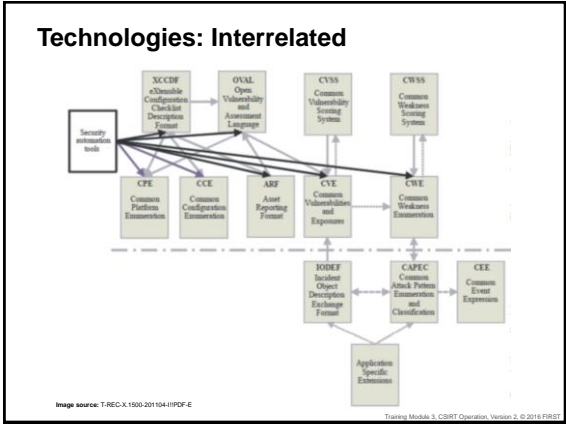
Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Technologies

- Information exchange
 - STIX
 - TAXII
 - IODEF
 - CVE
- Schema
 - CPE
 - OVAL
- Languages and protocols
 - SCAP



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST



Learning Check

Which types of security tools are the best kind of investment for your organization?

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Questions?

What questions do you have about this lesson?

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

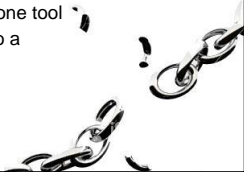
Section 3:
Identifying and Responding
to Attacks

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

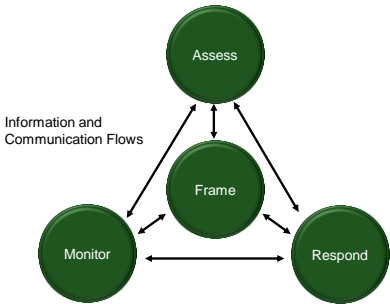
Exploiting Vulnerabilities

- Vulnerabilities: Errors that can be exploited
- Intersection of three elements:
 1. System susceptibility or flaw
 2. Attacker access
 3. Attacker capability
- An attacker must have at least one tool or technique that can connect to a system weakness

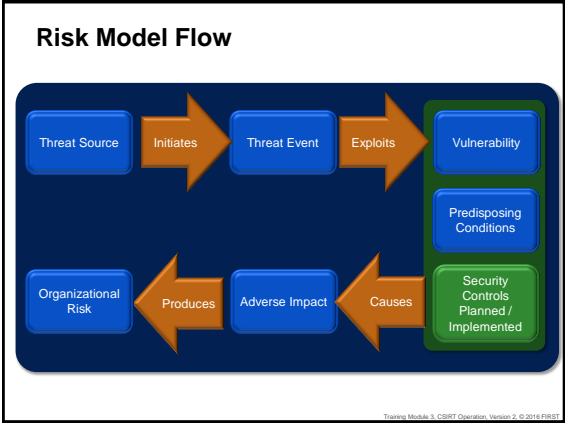
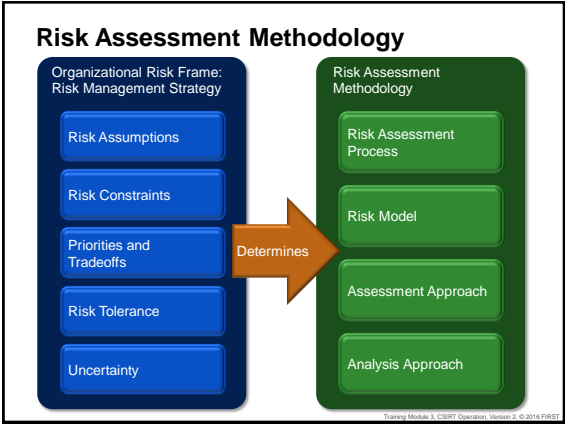
Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST




Risk Assessment




Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST



Assessing Risks



- ENISA risk assessment methods:
<http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-methods>
- ENISA risk assessment tools:
<http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-tools>
- ISO/IEC 2700x risk management standards:
<http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>



DoS/DDoS

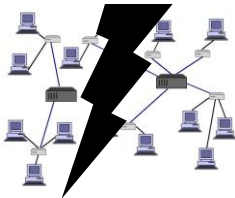
- Deliberate technical incidents
 - Overloading network access
 - Crashing the network
 - Exhausting resources
- Non-technical incidents
 - Breaches of physical security
 - Accidental damage to hardware
 - Extreme environmental conditions
 - System malfunctions
 - Uncontrolled system changes
- Botnet: Internet-connected computers that can be used for DDoS



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Other Types of Attacks

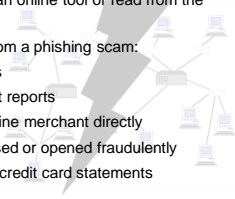
- Malware
- Website defacement
- Phishing
- Data breaches
- Target attacks and APTs



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Phishing and Email Headers

- Email headers determine where a message is sent and they record the path through each mail server
- Using online tools may give the manager of an email application total control over the email headers
- Read message headers by using an online tool or read from the bottom of the header
- Take steps to minimize damage from a phishing scam:
 - Change passwords or PINs
 - Place a fraud alert on credit reports
 - Contact the bank or the online merchant directly
 - Close any accounts accessed or opened fraudulently
 - Routinely review bank and credit card statements



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Learning Check

How do you weigh the impacts of different kinds of attacks?



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

How To Handle Attacks

- Put together an information security incident management policy
- A “kit” that allows consistent and appropriate responses to threats and closures of vulnerabilities



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

How To Handle Attacks: Policies

- Outline of the processes, responsible persons, authority, and reporting lines when a threat occurs
- Regular reviews
- Related awareness and training initiatives within the organization
- Directed at every person having legitimate access to its information systems and related locations
- Severity ratings for threats
- Suggested timeline for responding to attacks



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

How To Handle Attacks: Policies

- Identify:
- Objectives
 - Interested parties internally and externally
 - Vulnerabilities
 - Roles
 - Benefits



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Learning Check

What is the quality of your policies to handle attacks? What is the number one item you would like to add to your policies?



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Questions?

What questions do you have about this lesson?



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Section 4:
Communication

Training Module 3, CSIRT Operation, Version 1, © 2016 FIRST


Communication of Vulnerabilities
and Threats

- **Selected recipients:** Sending notifications only to recipients affected by the security vulnerability
 - Often used when an organization is small
 - Used when a product is a service
 - Can notify only customers that fit into a certain profile
- **Public notification:** Making notifications visible to all
 - Can identify all affected customers
 - Useful if products are sold via third parties
 - Any notification sent to customers
- Selected recipients or public notification based on ability to identify affected recipients and not mutually exclusive
- Can also group notifications by vulnerability

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Security Bulletin Format

- Consider medium, type, structure, and graphical layout:
 - Text, HTML, PDF, proprietary formats?
 - Free text, XML?
 - Email, Web, possibly RSS or product self-check?
- Contingency plan: CDs, DVDs, USBs



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Security Bulletin Language

- Make it bland and factual
 - Between formal and informal
 - Short sentences
 - Consistent expressions
 - Not too academic or technical
- If possible, translate into languages spoken by the majority of the customer base
 - Template text can help the translation
 - Point to the original English-language version



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Security Bulletins: Internal Review



- Security bulletin must be reviewed to ensure that it contains all the necessary information and is accurate
 - Developers
 - Customer support
 - Dedicated support people
 - Legal
 - PR
- CSIRT owns the security bulletin

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Security Bulletins: Push and Pull Notifications



- **Push model:**
 - Can be configured to suit recipients' needs
 - Can be sent to pagers, mobile phones, and email
- **Pull model:**
 - Device periodically checks for new security bulletins
 - Can automate the process of receiving and preprocessing the security bulletin
- Recipients nominate who receives security bulletins
- Security bulletins sent to everyone should be available without registration; security bulletins sent only to customers should require registration

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Security Bulletin Maintenance

- Decide:
- When to change the document revision number
 - Whether recipients need to be notified of the change
- Depends on:
- Which kinds of changes warrant a revision number
 - When recipients will be notified about changes



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Learning Check

What are some criteria that would increase the level of severity for a security bulletin?



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

In The News

- Sometimes an incident can put your organization front and center in the news
- What do you do?
- What protocols do you follow?



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Public Relations



- Turn all externally-facing communications over to your PR team
- Don't reach out to the press unless authorized
- Redirect press to appropriate PR staff
 - Prevents misinformation or speculation
 - Stays clear and concise
 - Aligns internal and external messages
- Your organization may designate you to speak

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Handling the Press

- Speak only if you are designated to speak to the press
- Only say what can be printed
- Prepare your answers
- Ask for questions in advance
- Only the truth
- Only the facts
- Create a "holding" statement
- Review the final article



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Learning Check

How does your organization handle incidents that involve the press?



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Questions?

What questions do you have about this lesson?



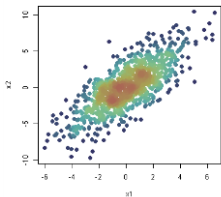
Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Section 5:
Testing, Verifying, and Improving
Your Process

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Ongoing Assessment

- Schedule regular checking and testing of information security incident management processes and procedures to highlight potential flaws and problems that can arise during the management of information security events, incidents, and vulnerabilities

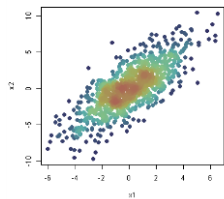


- Treat your CSIRT similar to a city emergency response team
- Foster smooth and effective communications between other teams, internally and externally

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Ongoing Assessment

- Check for trends and patterns that may help identify the need for controls or approach changes
- Conduct information security testing, particularly vulnerability assessment, following an IT-oriented information security incident
- Conduct vulnerability assessments on a regular basis, not just in response to incidents
- Regularly check and test processes and procedures around information security incident management



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Incident Response Mock Exercise Structure

- Goals:
 - Validation
 - Training
 - Testing
- Types of exercises:
 - Discussion-based
 - Tabletop
 - Live
 - Combination



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Incident Response Mock Exercise Structure

- Type of exercise depends on the goal and also available time and resources

Goal	Type of exercise
Validating new plans	discussion-based; tabletop
Training people	discussion-based; tabletop; live
Verifying validity of existing plans	tabletop; live

- Phases:
 - Planning and preparation
 - Execution
 - Debrief and post-mortem analysis



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Incident Response Mock Exercise Scope

- Scope considerations:
 - Internal, or internal and external?
 - Who needs to be involved?
 - How many exercise leaders are required?
- Important that all involved are aware that the scenario being handled is an exercise and not a real event



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Incident Response Mock Exercise Scope

- Guidelines:
- Brief participants on the exercise goals
 - Ensure safety and security of all participants
 - Make sure all participants know their roles
 - Ensure enough people to lead exercise
 - Allow sufficient time for discussion
 - Allow sufficient time and resources to debrief
 - Create and distribute exercise reports



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Incident Response Capability Monitoring

- Measure capabilities of the incident response team as well as related individuals and groups
- Capture:
 - Capabilities available to the organization
 - Who possesses them
 - Internal or external
 - How to engage
 - How current the capability is
 - How often the capability has been required



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Penetration Testing



- Simulated attack on a computer system to find vulnerabilities
- Improves the security of your company and increases security awareness of the staff
 - Performed in conjunction with IT department
 - Fixes assigned to appropriate parties
 - More testing performed after fixes applied

Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Learning Check

If you were going to do penetration testing, which of your applications or websites would you choose and why?



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST

Questions?

What questions do you have about this lesson?



Training Module 3, CSIRT Operation, Version 2, © 2016 FIRST