Module 3
CSIRT Operation Lab

Student Guide

Lab Introduction

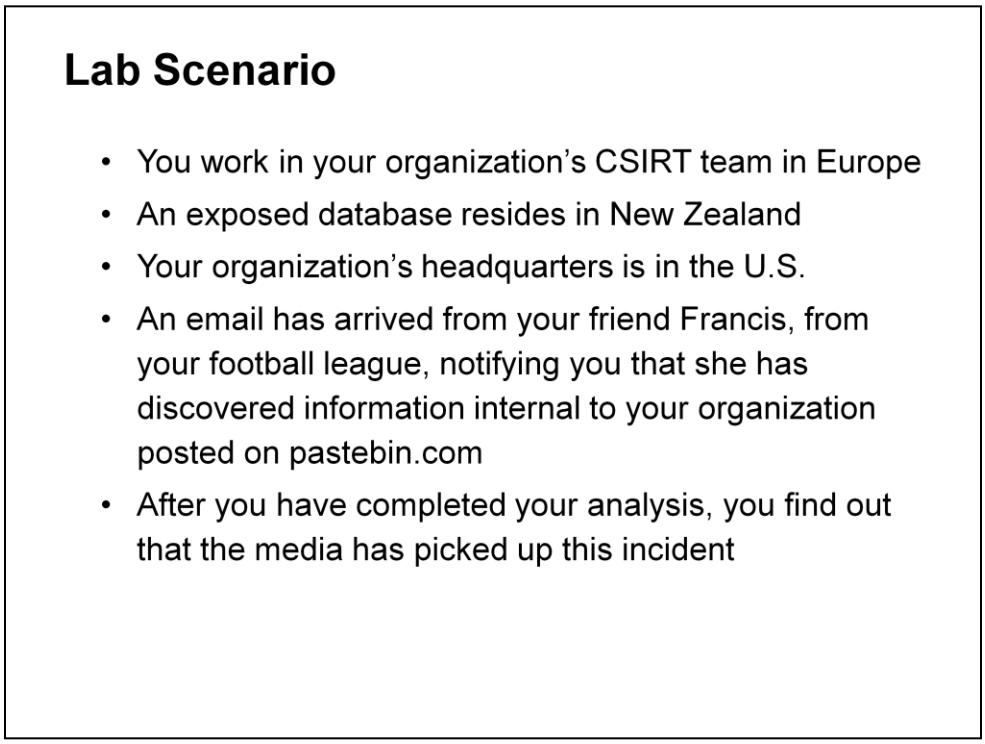
- Open your Lab Student Guide
- Your instructor will guide you through each step

Lab Introduction

We will take a simple scenario and move through the standard Incident Response steps, from the “Plan and prepare” phase to the “Conduct post-mortems and lessons learned sessions” phase, as a guided exercise that your instructor will lead. We will stop to ask and answer questions along the way.

Lab Steps: Incident Management Processes

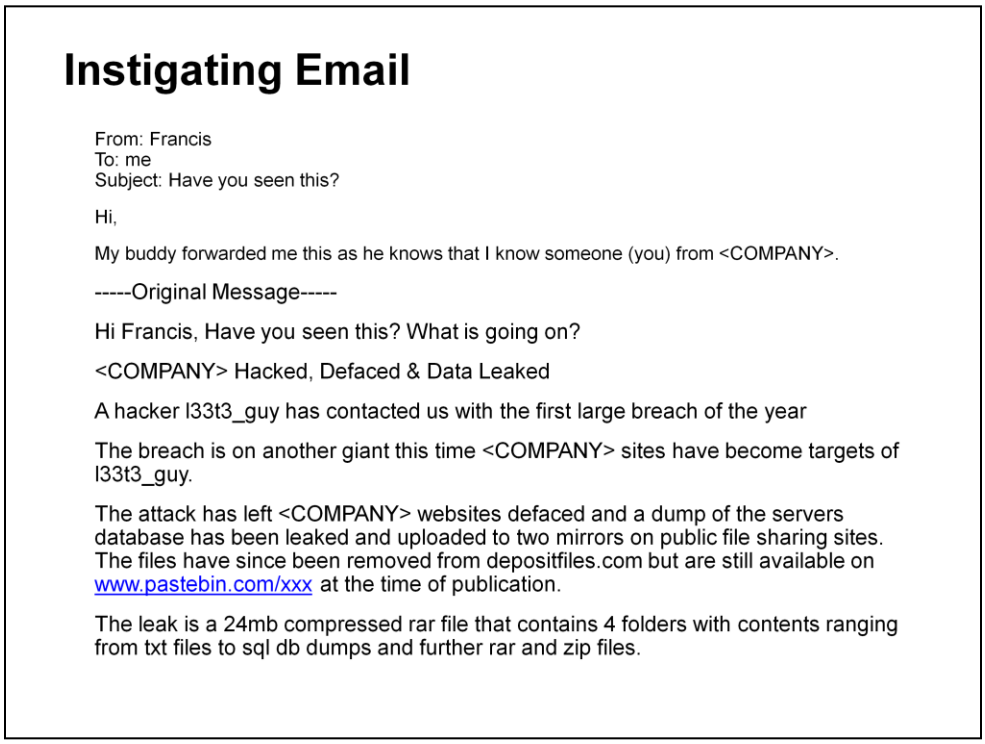
Use the Incident Response steps outlined in the course to develop an action plan for addressing this incident. At the end of this lab, you will have completed a full cycle of the standard Incident Response steps, working cooperatively with other teams in your organization and coordinating with outside organizations. We will follow all the steps we discussed during the lecture, including identifying any lessons learned to improve our processes. You may address any variety of solutions and use information about your organization to customize your specific policies and processes.



Lab Scenario

Here's the scenario:

- You work in your organization's CSIRT team, which is based in Europe.
- An exposed database resides in New Zealand.
- Your organization's headquarters is in the U.S.
- An email has arrived from your friend Francis, from your football league, notifying you that she has discovered a number of email addresses and some other information internal to your organization posted on pastebin.com.
- After you have completed your analysis, you find out that the media has picked up this incident, and the organization has to respond to public relations (PR) requests, and/or (optionally) to proactively reach to media.



Instigating Email

This is an email from your friend Francis forwarding an email that was forwarded to her.

Sample of pastebin.com Contents

file1.txt

ID	jmeno	email	heslo	login	prijmeni	vyrobek	rowguid
14	Daniel	prentis@kaktus.mx			p	prentis	Prentis B56778DF-8C6E-4E4E-B3AC-09ABF55CCC5F
15	gggg	fffff	a	admin	fffffff		C3D23D86 . . .
17	f	f	f	f	f	f	0615821E . . .
16	q	q	q	q	q	q	85FC2FD6 . . .
20	Jan	zich@kaktus.mx	disevycpat			janzich	Zich . . .

file2.txt

id	jmeno	prijmeni	email	mesto	ulice	psc	telefon	pohlavi
	rokNarozeni		login	heslo				
3	test	test	j.pavlik@kaktus.mx			ccc	xxx	100
	123	0	222	test	123456			
20	Eduard	Mácha	e.macha@kaktus.mx				Ostrava	Na skotnici
304	111 05	606742819		1	1969	macho	molly	

Sample of pastebin.com Contents

This is a sample of the output. Ask your instructor where to find the pastebin.com files file1.txt and file2.txt related to this lab.

CSIRT Contacts

Here is the full list of the relevant contacts in your CSIRT departmental contact list.

Internal Contacts:

- Legal: Leslie Lu, based in London, U.K.
- PR: Patrick Pan, based in Palo Alto, U.S.
- DB contact: Devi Dharma, based in New Zealand

External Contacts:

- Media contact: Milli Massimo, *The Local Times*, a local acquaintance
- Administrator at pastebin .com: Amir Au

Information on exposures:

- Daniel Prentis, prentis@kaktus.mx and Jan Zich, zich@kaktus.mx are internal employees of your organization. They reside in Ireland and Germany, respectively.
- J. Pavlik, j.pavlik@kaktus.mx does not work for your company. She resides in the U.S.
- Eduard Ostraa Na, e.macha@kaktus.mx does not work for your company. He resides in xxxxx

For country by country laws, check the Global Guide to Breach Notifications at:
http://www.theworldlawgroup.com/wlg/Global_Data_Breach_Guide_Home.asp

Answers and Follow-up Discussions

Answers and Follow-up Discussions

Once we have completed the exercise, we will discuss the answers so you can learn more from others in the class.

And now, let’s get started!

Step 1: Plan and Prepare

a. What are the three key relationships within your organization?
b. Are there any you still need to establish?
c. What are your three key external relationships?

Step 1. Plan and Prepare

This phase is addressed after post-mortem completion and periodically, over time.

a. For the CSIRT within your organization, list your three key organizational relationships.

_____
_____
_____

b. Are there any relationships you still need to establish?

_____
_____

c. What are your three key external relationships?

_____
_____

Step 2: Detect

a. From whom did you get the suspected incident? What that person internal or external?
b. What information in the files might be sensitive?
c. What information do you need to collect to perform triage?
d. What digital evidence can you collect? Where should you store it? Do you have a policy at your organization?

Step 2. Detect

During the Detect phase, an incident can be either discovered by your team or reported to your team.

a. From whom did you get this suspected incident? Was that person or team internal or external to your organization?

_____

b. What information in these files might be sensitive?

_____

c. What information do you need to collect from these emails to appropriately triage the incident? Is your pastebin.com Administrator contact information current?

_____

d. What digital evidence can you collect? Does your organization have a policy about where to store evidence? If not, what policy do you think you should institute?

_____
_____

Step 3: Triage

a. How does this incident impact your organization?
b. What severity would be assigned? What incidents have higher priority? Lower?
c. What might have higher urgency? Lower urgency?
d. In your organization, how are urgency level defined?

Step 3. Triage

The Triage phase assures that your CSIRT team is working on the highest-risk threats first. This is based on the initial data (if there is any) for this incident.

a. How does this incident impact your organization?

_____
_____

b. Based on your organization's policies, what severity would be assigned? What types of incidents would have higher priority? What types of incidents would have lower priority?

_____
_____
_____

c. Based on your organization's policies, what types of incidents might be of higher urgency? What types of incidents might be of lower urgency?

_____
_____
_____

d. Within your organization, are urgency levels defined by policy or are they set dynamically? If dynamically, are they set by a manager or someone other than your team?

_____
_____

Step 4: Analyze

a. What are your first steps?

Step 4. Analyze

Once this incident is high enough in the queue, your CSIRT team will perform an in-depth review and come up with conclusions. During this phase it is likely that you will be working with other teams, both internal to your organization and possibly externally.

a. What are your first steps?

_____

_____

_____

Step 4: Analyze

a. What are your first steps?
b. What are your conclusions?
c. What teams did you work with in this phase?

Step 4. Analyze (continued)

b. What are your conclusions from this investigation?

_____
_____
_____

c. What are all the teams you worked with in this phase?

_____
_____
_____

Step 5: Respond

a. What steps do you need to take to clean up the attack?
b. Who do you need to contact, internally and externally?

Step 5. Respond

In this phase you will close out this incident, contacting internal and external teams and media as appropriate to the situation.

a. What steps do you need to take to clean up the attack?

_____
_____
_____

b**.** Who do you need to contact, both internally and externally?

_____
_____
_____

Consider the following contacts:

- Your organization's Legal Department, Leslie Lu
- Your organization's PR department, Patrick Pan
- Other departments within your organization
- Your media friend, Milli Massimo
- Your close family – because it was a really interesting attack

Step 5: Respond

a. What steps do you need to take to clean up the attack?
b. Who do you need to contact, internally and externally?
c. How does your internal communications plan differ from your external plan?
d. For your organization, do you involve Legal and PR?
e. What actions do you need to take in addition to contacted the affected individuals?
f. What did you do when you found out Leslie Lu had left the company?

Step 5. Respond (continued)

c. Does your internal communications plan differ from your external plan? If so, in what way?

_____

d. Should you contact the affected individuals directly or involve Legal and PR? Why or why not?

_____

_____

e. What actions do you need to take in addition to contacting the affected people?

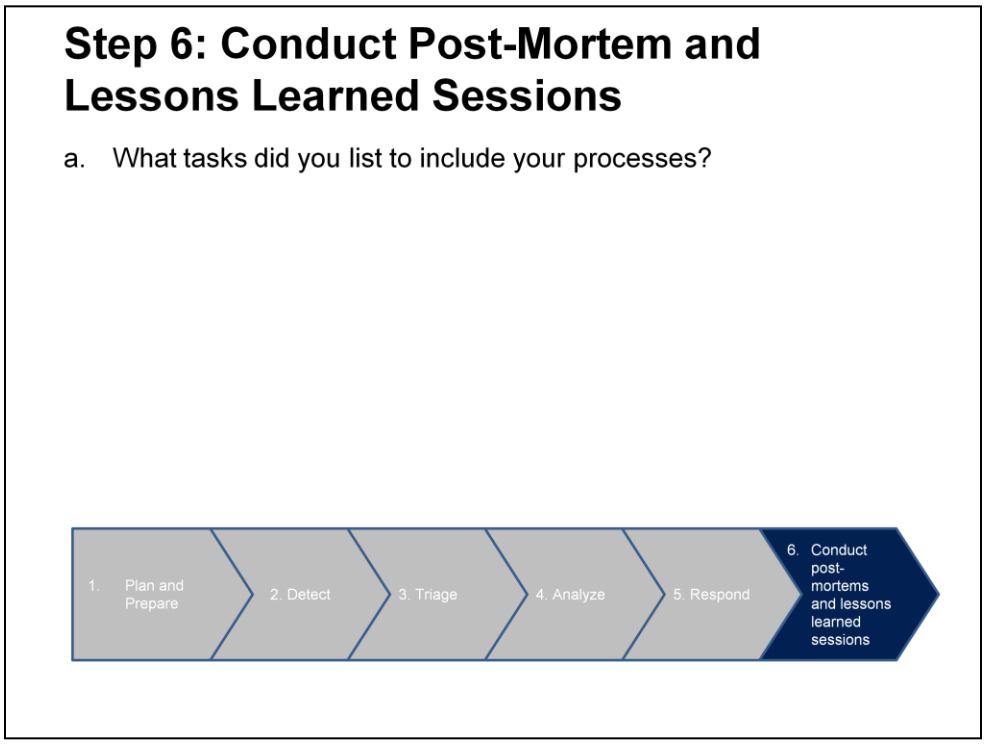
_____

_____

f. Whoops!! When you tried to contact Leslie Lu, of Legal, you found out she has left the company. What should you do next?

_____

_____



Step 6. Conduct Post-Mortem and Lessons Learned Sessions

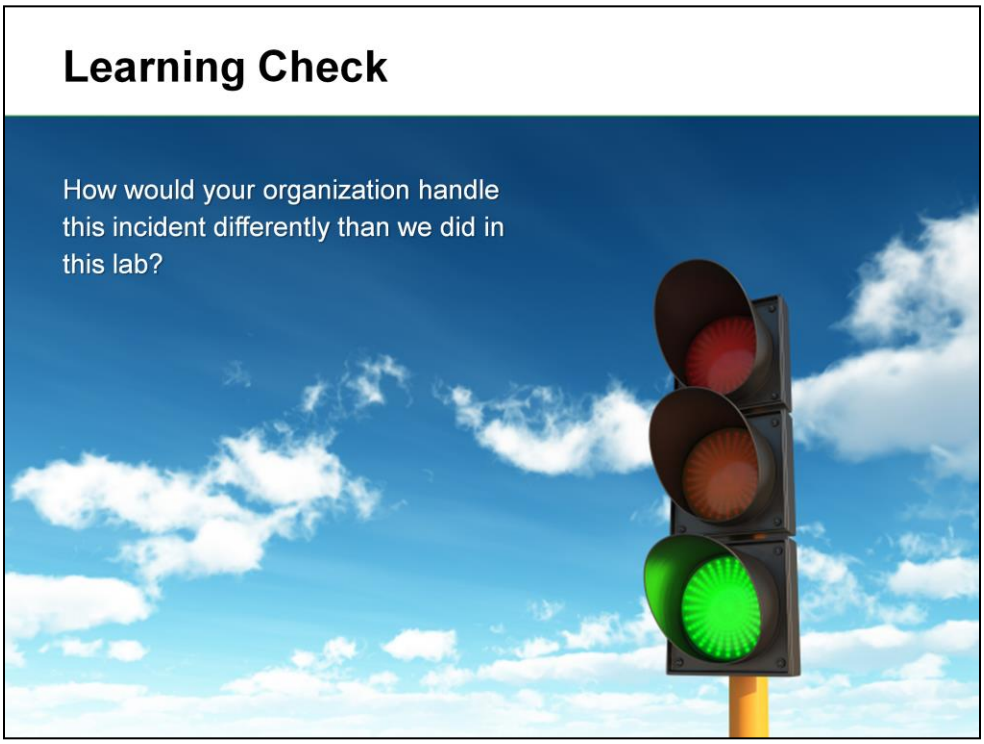
You should perform a post-mortem periodically for all events that have occurred since the last PM to identify lessons learned and develop best practices.

a. Develop an action plan for how to improve your processes.

_____

_____

_____



Learning Check

Thinking about your role, how do you think you might have handled this incident differently in your organization? How would your organization expect you to handle it?


FIRST
Improving Security Together