FUNDAMENTALS OF INCIDENT HANDLING

MONDAY 24 - FRIDAY 28 OCTOBER 2011

SOFTWARE ENGINEERING INSTITUTE

The Carnegie Mellon Software Engineering Institute (SEI) works closely with defense and government organisations, industry, and academia to continually improve software-intensive systems. Our core purpose is to help organisations improve their software engineering capabilities and to develop or acquire the right software, defect free, within budget and on time, every time.

For more information on the Software Engineering Institute Program, visit www.cmu.edu.au/sei

ABOUT THE COURSE

This five-day course is for computer security incident response team (CSIRT) technical staff who have little or no incident handling experience. It provides a basic introduction to the main incident handling tasks and critical thinking skills that will help an incident handler perform their daily work. It is recommended to those new to incident handling work.

The course is designed to provide insight into the work that an incident handler may perform. It will provide an overview of the incident handling arena, including CSIRT services, intruder threats, and the nature of incident response activities.

Course attendees will learn how to gather the information required to handle an incident; realise the importance of having and following pre-defined CSIRT policies and procedures; understand the technical issues relating to commonly reported attack types; perform analysis and response tasks for various sample incidents; apply critical thinking skills in responding to incidents, and identify potential problems to avoid while taking part in CSIRT work. The course incorporates interactive instruction, practical exercises, and role playing. Attendees have the opportunity to participate in sample incidents that they might face on a day-to-day basis.

This course is part of the curriculum for the CERT-Certified Incident Handler program. After completing this course, participants are encouraged to attend the companion course, Advanced Incident Handling.

WHO SHOULD ATTEND?

• New CSIRT technical staff (one to three months of experience)
• Experienced CSIRT staff who would like to benchmark their CSIRT processes and skill sets against best practices
• Anyone who would like to learn about basic incident handling functions and activities

TOPICS

• Understanding the CSIRT environment and basic incident management processes
• CSIRT code of conduct
• Understanding security tools and technologies used by CSIRTs
• Identifying and gathering critical information
• Recognising signs of attacks
• Detecting and analysing incidents
• Finding contact information
• Coordinating response and disseminating information
• Handling email and malicious code attacks
• Working with law enforcement

OBJECTIVES

This course will help participants to
• Recognise the importance of following well-defined processes, policies, and procedures
• Understand the technical, communication, and coordination issues involved in providing a CSIRT service
• Critically analyse and assess the impact of computer security incidents
• Effectively build and coordinate response strategies for various types of computer security incidents

PREREQUISITES
Before registering for this course, participants must be familiar with Internet services and protocols.
It is recommended but not required that participants have some experience with system administration for Windows or UNIX systems.

MATERIALS
Participants will receive a course notebook and a CD containing the course materials.

VENUE
Carnegie Mellon University - Australia
220 Victoria Square (Torrens Building), Adelaide

COST
Tuition AUD $5,425 incl. GST
AUD $4,900 incl. GST for government employees
Cancellation fee of AUD $500 will apply 10 days prior to course commencement. Name changes permitted if you are unavailable to attend.

REGISTER TODAY
T +61 (0) 8 8110 9910
E admissions@cmu.edu.au
F +61 (0) 8 8211 9444
W www.cmu.edu.au/sei

PROGRAM SCHEDULE

<table>
<thead>
<tr>
<th>Date</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday 17 October</td>
<td>Participants receive pre-course reading materials</td>
</tr>
<tr>
<td>Monday 24 October</td>
<td>9am – 5pm Course commences (meals &amp; refreshments included)</td>
</tr>
<tr>
<td>Tuesday 25 October</td>
<td>9am – 5pm Course continues (meals &amp; refreshments included)</td>
</tr>
<tr>
<td>Wednesday 26 October</td>
<td>9am – 5pm Course continues (meals &amp; refreshments included)</td>
</tr>
<tr>
<td>Thursday 27 October</td>
<td>9am – 5pm Course continues (meals &amp; refreshments included)</td>
</tr>
<tr>
<td>Friday 28 October</td>
<td>9am – 5pm Course concludes (meals &amp; refreshments included)</td>
</tr>
<tr>
<td>SURNAME</td>
<td>FIRST NAME</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TITLE</th>
<th>EMAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ORGANISATION</th>
<th>ORGANISATION ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>POSTAL ADDRESS FOR INVOICE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PHONE</th>
<th>FAX</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MOBILE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

**PLEASE LET US KNOW IF YOU HAVE ANY SPECIAL REQUIREMENTS INCLUDING: DIETARY, MOBILITY ACCESS OR OTHER.**

**PLEASE CHECK IF YOU DO NOT WANT YOUR NAME AND CONTACT INFORMATION TO APPEAR ON THE CLASS PARTICIPATION LIST.**

**WE WILL PROVIDE YOU WITH TAX INVOICE AND PAYMENT DETAILS UPON RECEIPT OF YOUR REGISTRATION FORM**

**QUESTIONS ABOUT THE PROGRAM**

**Carnegie Mellon University - Australia**

Anna Cosentino  
Chief Operating Officer  
T +61 8 8110 9905  
M 0403 602 374  
E acosenti@cmu.edu.au  
W www.cmu.edu.au/sei

220 Victoria Square  
Adelaide, South Australia 5000 Australia

**TO REGISTER**

Admissions Office  
T +61 (0) 8 8110 9910  
E admissions@cmu.edu.au  
F +61 (0) 8 8110 9444  
W www.cmu.edu.au/sei