Learning objectives
Upon completion of this course, students will be able to:
• Understand the basic theories of implementing a defence in depth program.
• Identify potential risks when using a non-secure system.
• Identify potential attacks used by hackers
• Execute system hardening
• Know the concepts of Domain and Workgroup environments
• Execute basic system hardening
• Configure the Windows Update using the off-line and on-line available tools
• Configure the Antivirus Update using the off-line and on-line available tools
• Configure Symphony Plus Users
• Familiarize with ABB’s CSWP tool
• Use CSWP Antivirus management module
• Use CSWP Patches management module
• Use CSWP Hardening module
• Use CSWP Backup & Restore module
• Use CSWP Reports, Events & Logs module

Prerequisites
Students should have strong knowledge of Windows Operating Systems, TCP/IP Networks, and Microsoft Active Directory administration and troubleshooting.

Topics
• Introduction to Cyber Security
• Cyber Attack Overview
• IT/OT Network and security weakness
• System Hardening - Services
• System Hardening - Firewall
• System Hardening - Policy
• System Hardening - Miscellaneous
• AD & DS - Security
• Windows Update - WSUS
• Antivirus Update - McAfee
• Symphony Plus User Management
• Overview of CSWP
• CSWP Requirement & Specification
• CSWP - Antivirus Management
• CSWP - Patches Management
• CSWP - Hardening: Services, Ports, Firewall
• CSWP - Backup & Restore
• CSWP - Report & Events & Logs

Participant profile
This training is targeted to system and application engineers, commissioning and maintenance personnel, service engineers and system integrators.

Course type and methods
This is an instructor led course with interactive classroom discussions and associated lab exercises. Approximately 50% of the course is hands-on lab activities.

Duration
4 1/2 days
### Agenda

<table>
<thead>
<tr>
<th>Day 1</th>
<th>Day 2</th>
<th>Day 3</th>
<th>Day 4</th>
<th>Day 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course overview</td>
<td>System Hardening - Services</td>
<td>Antivirus Update - McAfee</td>
<td>CSWP - Patches Management</td>
<td>CSWP - Report &amp; Events &amp; Logs</td>
</tr>
<tr>
<td>Cyber Security on Industrial Control Systems (ICS)</td>
<td>System Hardening - Policy</td>
<td>Overview of CSWP</td>
<td>CSWP - Backup and Restore</td>
<td>Questions &amp; Answers</td>
</tr>
<tr>
<td>Cyber Attack Overview</td>
<td>S+ Hardening - Misc.</td>
<td>CSWP Requirement &amp; Specification</td>
<td>Hands-on lab: exercises</td>
<td></td>
</tr>
<tr>
<td>IT/OT Network and security weakness</td>
<td>AD &amp; DS - Security</td>
<td>CSWP - Antivirus Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hands-on lab: exercises</td>
<td>Windows Update - WSUS</td>
<td>Hands-on lab: exercises</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

The information contained in this document is for general information purposes only. While ABB strives to keep the information up to date and correct, it makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the information, products, services, or related graphics contained in the document for any purpose. Any reliance placed on such information is therefore strictly at your own risk. ABB reserves the right to discontinue any product or service at any time. © Copyright 2018 ABB. All rights reserved.