

## Course Outline

Security Center: System Hardening certification	
<b>Code</b>	SC-SHC-001
<b>Level</b>	Intermediate
<b>Duration</b>	2 hours (self-paced, online training)
<b>Target audience</b>	Technicians, Administrators, and IT Professionals
<b>Prerequisites</b>	Successful completed of the SC-OTC-001, SC-STC-001, SC-AFC-001 or SC-AMP-001 certification training
<b>Objectives</b>	<ul style="list-style-type: none"><li>• Understand the growing risks of the interconnected world</li><li>• Understand the impact and risk on security systems</li><li>• Understand Genetec's approach to system security</li><li>• Apply a practical analysis using access control as an example</li><li>• Use security hardening tools built-in to Security Center</li><li>• Apply general best practices to a Security Center system</li><li>• Understand the direction needed going forward</li></ul>
<b>Certification</b>	Yes. Online quiz

Topic	Description
<b>Module 0:</b> <i>Introduction</i>	<ul style="list-style-type: none"> <li>• Introduction</li> <li>• What to expect in this training</li> </ul>
<b>Module 1:</b> <i>The growing risks of our interconnected world</i>	<ul style="list-style-type: none"> <li>• The price of interconnectivity</li> <li>• The cost of cyber threats</li> <li>• Recent cyber events and statistics</li> </ul>
<b>Module 2:</b> <i>Why should I care?</i>	<ul style="list-style-type: none"> <li>• What is the risk to video surveillance systems?</li> <li>• IoT attacks</li> <li>• Untrusted devices</li> <li>• Lateral movement</li> <li>• What is the risk to access control systems?</li> </ul>
<b>Module 3:</b> <i>Approach to system hardening.</i>	<ul style="list-style-type: none"> <li>• Security of your security system               <ul style="list-style-type: none"> <li>○ Authentication</li> <li>○ Authorization</li> <li>○ Encryption</li> </ul> </li> </ul>
<b>Module 4:</b> <i>Practical hardening analysis</i>	<ul style="list-style-type: none"> <li>• Practical analysis (access control)</li> <li>• Architecture</li> <li>• Credentials</li> <li>• Wiegand vs OSDP</li> <li>• TLS</li> <li>• Secure architecture</li> </ul>
<b>Module 5:</b> <i>Security Center hardening</i>	<ul style="list-style-type: none"> <li>• Security Score widget</li> <li>• Firmware vault</li> <li>• Privilege troubleshooter</li> <li>• 11 “best practices”</li> </ul>
<b>Module 6:</b> <i>Next steps</i>	<ul style="list-style-type: none"> <li>• Choose certified solutions</li> <li>• Cybersecurity is everyone’s concern, not just IT</li> <li>• Educating users is key</li> <li>• Reference info / documentation</li> </ul>
<b>SC-SHC-001 Certification test</b>	<ul style="list-style-type: none"> <li>• A certification Exam will be given at the end of this course.</li> <li>• A total score of 80% or better is required to pass.</li> </ul>