Cybersecurity Education Catalog
Introduction

The human factor – what employees do or don’t do – is the biggest vulnerability to an organization’s information security, yet it’s often the most overlooked. Whether they are processing credit cards, handling clients’ personal information, or developing software solutions for your business, your employees are ripe targets for information thieves seeking access to your sensitive data, unless you help them learn how to protect against and respond to security incidents. It’s vital to your business to provide security education to your employees and partners.

Trustwave offers two key types of Cybersecurity Education:

- Security Awareness Education for all staff
- Secure Developer Training for technical staff

Use this catalog to browse the Cybersecurity Education offerings. If you have questions, reach out to your Trustwave account manager or use the Contact Us section of the Trustwave website at www.trustwave.com.
# Table of Contents

**Security Awareness Education (SAE)** ______________________________ 2  
- SAE Courses ___________________________________________ 3  
- Security Awareness Curriculum Builder ______________________ 6  
- SAE Course Bundles ______________________________________ 8  
- SAE Supplemental Training _________________________________ 10

**Secure Development Training (SDT)** ____________________________ 11  
- SDT Courses ____________________________________________ 12  
- SDT Course Bundles ______________________________________ 20
Security Awareness Education

Every Trustwave Security Awareness Education (SAE) program is customized for you, the client. Your options include how your online security education courses will be set up and which additional video and print-based materials you would like to order to reinforce your program year-round. This section is designed to guide you through the program and help you choose the options that are right for you and your organization.

SAE Courses
Use the SAE Courses list to browse our library of security awareness courses. Categorized by areas of interest, each course’s catalog code, topic, and objectives are listed to help you decide which topics are most appropriate for your target audience(s). All courses are available in English. Most courses are available in German and Spanish, and all courses can be localized into additional languages. The portal is English by default and may be configured in Spanish, French and Portuguese as well as many other languages. You may also view our courses in the Trustwave Cybersecurity Education portal. Contact your Trustwave account manager if you would like to receive a free trial.

Security Awareness Curriculum Builder
The Security Awareness Curriculum Builder page lists the courses included in each available curriculum, tailored for common organizational roles requiring security awareness training. If these combinations don’t fit your organization’s needs, or if you’d like to include additional materials such as quizzes or your organization’s own information security policies, use the table at the bottom of the Security Awareness Curriculum Builder page to identify the curriculum you would like us to build.

Supplemental Material to Support Security Awareness
Often organizations administer formal security awareness training only once per year. Hanging posters in your office environment and featuring the two-minute security videos in public areas and meetings can help keep employees aware of their security responsibilities year-round.
SAE Courses

Each curriculum in your Security Awareness Education program may be comprised of one or more of the following courses. Use this guide to identify the courses you would like to include in each curriculum. If you have any questions, or if you would like to receive a free trial, contact your Trustwave account manager.

**Compliance Topics**  These courses present the basic principles of various compliance standards and information security measures.

<table>
<thead>
<tr>
<th>#</th>
<th>Course Name</th>
<th>Course Objectives</th>
<th>Supporting Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWA 001</td>
<td>Introduction to the PCI DSS Compliance Standard</td>
<td>Recognize how the Payment Card Industry Data Security Standard (PCI DSS) protects cardholder data.</td>
<td>• Identify elements of cardholder data that must be protected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Recognize appropriate protection mechanisms for cardholder data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Describe the continuous process to maintain PCI compliance.</td>
</tr>
<tr>
<td>AWA 002</td>
<td>PCI for Business as Usual (BAU) Compliance</td>
<td>Understand best practices to implement PCI DSS controls and make compliance business as usual.</td>
<td>• Understand the “big picture” purpose of the PCI DSS to protect the business and serve customers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Acknowledge the importance of data security measures to achieve compliance and maintain security.</td>
</tr>
<tr>
<td>AWA 015</td>
<td>PCI Compliance</td>
<td>Understand the importance of the Payment Card Industry Data Security Standard (PCI DSS).</td>
<td>• Recognize appropriate protection mechanisms for cardholder data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Recognize how the PCI DSS helps minimize risk to cardholder data.</td>
</tr>
</tbody>
</table>

**Security Awareness Topics**  These courses present basic security awareness concepts that all employees should understand.

<table>
<thead>
<tr>
<th>#</th>
<th>Course Name</th>
<th>Course Objectives</th>
<th>Supporting Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWA 004</td>
<td>Introduction to Security Awareness</td>
<td>Create awareness of best practices for protecting sensitive information, how to handle information securely and the risks of mishandling information.</td>
<td>• State how actions can impact the security of your organization and identify what criminals are after.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Provide examples of sensitive information in the workplace and how to categorize it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Define PII, identify examples of it and state how to protect your information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Be aware of how information is protected, including data integrity.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Describe benefits of security awareness and apply what you have learned to avoid becoming a victim.</td>
</tr>
<tr>
<td>AWA 007</td>
<td>Information Privacy and Security Awareness for Executives</td>
<td>Provide decision-makers and managers with a concise summary of essential information privacy and security awareness requirements.</td>
<td>• Learn how to identify, help prevent and defend against the most common privacy and security threats.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Recognize the importance of understanding what constitutes private data.</td>
</tr>
<tr>
<td>AWA 008</td>
<td>Information Privacy - Classifying Data</td>
<td>Recognize the importance of understanding what constitutes private data.</td>
<td>• Recognize the importance of meeting internal and external security compliance requirements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Understand how to classify data based on sensitivity level and risk.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Learn best practices for protecting sensitive data.</td>
</tr>
<tr>
<td>AWA 009</td>
<td>Information Privacy - Protecting Data</td>
<td>Recognize the importance of understanding what constitutes private data and how to behave in a proactive manner to protect this information in everyday work.</td>
<td>• Understand physical controls, technical controls and administrative policies and and practices in support of data privacy.</td>
</tr>
</tbody>
</table>

A video related to this course topic is available.
## Security Awareness Topics

These courses cover basic security awareness concepts that all employees should understand.

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Description</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWA 010</td>
<td>Email Security</td>
<td>Recognize malicious email before it can become a threat.</td>
<td>• Learn how to properly handle email.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Learn best practices around how and when to use email to send specific types of information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Understand what Personally Identifiable Information (PII) is.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Understand the impact of sending sensitive information over an insecure medium.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Identify information that should not be sent via email.</td>
</tr>
<tr>
<td>AWA 012</td>
<td>Malware Awareness</td>
<td>Learn how to identify and define types of malware.</td>
<td>• Recognize evidence of active infection and understand what the proper actions are to prevent such attacks.</td>
</tr>
<tr>
<td>AWA 013</td>
<td>Mobile Security</td>
<td>List the characteristics of mobile device platforms.</td>
<td>• Identify the role device ownership plays as a basis for understanding application risk.</td>
</tr>
<tr>
<td>AWA 014</td>
<td>Password Security</td>
<td>Learn how to create and remember strong passwords, therefore eliminating the need to use insecure practices.</td>
<td>• Recognize the risks surrounding password security.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Identify safeguards used to protect passwords.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Summarize techniques used by attackers to obtain passwords.</td>
</tr>
<tr>
<td>AWA 016</td>
<td>Phishing Awareness</td>
<td>Recognize malicious email before it can become a threat.</td>
<td>• Understand the various ways in which attackers try to trick and entice users to trigger malicious events through email.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Learn best practices to properly handle and avoid phishing attacks.</td>
</tr>
<tr>
<td>AWA 017</td>
<td>Physical Security</td>
<td>Learn accepted practices for minimizing breaches and identifying different types of data that may be exposed via hardware theft.</td>
<td>• Understand what physical security is and why it is everyone’s responsibility.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Identify common physical security attacks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Identify physical security best practices.</td>
</tr>
<tr>
<td>AWA 018</td>
<td>Social Engineering Awareness</td>
<td>Identify the many forms of social engineering and its potential impacts.</td>
<td>• Identify techniques used by social engineers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Understand how to establish validity of requests in order to perform daily business functions in light of potential threats.</td>
</tr>
<tr>
<td>AWA 019</td>
<td>Travel Security</td>
<td>Recognize the risks associated with transporting sensitive data.</td>
<td>• Recognize threats that may be present while traveling.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Identify the risks certain locations may harbor.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Understand the defenses that you may employ while traveling.</td>
</tr>
</tbody>
</table>
### Best Practices for Job Roles
These courses target specific job roles within an organization. Each course you create should contain one of these JRT (Job Role Training) lessons, depending on your role and industry.

<table>
<thead>
<tr>
<th>#</th>
<th>Course Name</th>
<th>Course Objectives</th>
<th>Supporting Objectives</th>
</tr>
</thead>
</table>
| JRT 001 | Secure Practices for Retail Associates | Recognize the security awareness responsibilities of retail associates and the laws, regulations, methods and best practices that help keep information secure in the retail environment. | • Recognize the information security responsibilities of retail associates that impact the retail environment.  
• List and describe information security responsibilities and best practices of retail associates. |
| JRT 002 | Secure Practices for Retail Managers | Recognize the security awareness responsibilities of retail managers and the laws, regulations, methods and best practices that help keep information secure in the retail environment. | • Recognize the security responsibilities of retail managers or owners that impact the retail environment.  
• List and describe information security responsibilities and best practices of retail managers. |
| JRT 003 | Secure Practices for Call Center Associates | Recognize the security awareness responsibilities of call center employees and the laws, regulations, methods and best practices that help to keep information secure. | • Recognize the information security laws and regulations that impact the call center environment.  
• Recognize the responsibility of call center employees to protect the information they work with each day.  
• List and describe the information security responsibilities and best practices of call center employees. |
| JRT 004 | Secure Practices for Call Center Managers | Recognize the security awareness responsibilities of call center managers and the laws, regulations, methods and best practices that help keep information secure in the call center. | • Recognize the information security responsibilities of call center managers and the related laws and regulations that impact the call center environment.  
• List and describe information security responsibilities and best practices of call center managers. |

### Advanced Security Topics
These courses cover a wide range of advanced topics for managers and technical personnel.

<table>
<thead>
<tr>
<th>#</th>
<th>Course Name</th>
<th>Course Objectives</th>
<th>Supporting Objectives</th>
</tr>
</thead>
</table>
| ADV 002 | Exploring Security Trends     | Learn about the Global Security Report (GSR), recognize the sources of information reported, and review the findings of Trustwave's team of security experts. You will also be introduced to key themes and recommendations based on security trends. | • Describe what the Global Security Report is and recognize its benefits.  
• Identify what criminals are targeting the most and list the type of data targeted by cybercriminals.  
• Discuss what industries cybercriminals were targeting and which one was hit the hardest.  
• Discuss compromises by environment and what you can do to prevent compromises.  
• Reflect upon the global conclusion and 10 year summary and how this information impacts your business and personal information. |
### Security Awareness Education Curriculum Builder

The first table below is a list of curriculum recommendations for common job roles that fit most organizations. It shows the courses included for each recommended curriculum. If you prefer to create a custom curriculum, use the Create Your Own table to indicate what courses you would like to include.

The video list on the next page indicates which two-minute videos are associated with which curriculum.

<table>
<thead>
<tr>
<th>Course</th>
<th>AWA 001</th>
<th>AWA 002</th>
<th>AWA 004</th>
<th>AWA 006</th>
<th>AWA 008</th>
<th>AWA 009</th>
<th>AWA 010</th>
<th>AWA 012</th>
<th>AWA 013</th>
<th>AWA 014</th>
<th>AWA 015</th>
<th>AWA 016</th>
<th>AWA 017</th>
<th>AWA 018</th>
<th>JRT 001</th>
<th>JRT 002</th>
<th>JRT 003</th>
<th>JRT 004</th>
<th>ADV 022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and Privacy Awareness for Executives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security and Privacy Awareness for General Staff</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security and Privacy Awareness for Retail Associates</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security and Privacy Awareness for Retail Managers</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security and Privacy Awareness for Call Center Associates</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security and Privacy Awareness for Call Center Managers</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security and Privacy Awareness for Compliance Managers</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCI Fundamentals</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Data Protection Regulation (GDPR)</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced Topics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Create your Own

Use this section to mix and match lessons to build up to three courses of your own. Just print this sheet and fill in the necessary information, which you can then share with your Trustwave account manager.
Security Awareness Education Curriculum Videos

See the list below to determine which two-minute videos are included in which curriculum. You can add any videos to any curriculum you want.

<table>
<thead>
<tr>
<th>Video Title</th>
<th>VID 001</th>
<th>VID 002</th>
<th>VID 003</th>
<th>VID 004</th>
<th>VID 005</th>
<th>VID 006</th>
<th>VID 007</th>
<th>VID 008</th>
<th>VID 009</th>
<th>VID 010</th>
<th>VID 011</th>
<th>VID 012</th>
<th>VID 013</th>
<th>VID 014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and Privacy Awareness for General Staff</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Security and Privacy Awareness for Retail Associates</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Security and Privacy Awareness for Retail Managers</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Security and Privacy Awareness for Call Center Associates</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Security and Privacy Awareness for Call Center Managers</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Security and Privacy Awareness for Compliance Managers</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>PCI Fundamentals</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>General Data Privacy Regulation (GDPR)</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>
Role-Based Security Awareness Education

Here is a list of curriculum recommendations for common job roles. Each curriculum is available for you to assign to your employees using the Learning Assignment Tool in the Cybersecurity Education portal. If you prefer to create your own curriculum with a custom set of courses, please contact your Trustwave account manager.

Security and Privacy Awareness for Executives (55 minutes)
Course Code: SAE EXEC
This course is designed for executives who want an overview of information privacy and security awareness.
- AWA 007 Information Privacy and Security Awareness for Executives (45 minutes)
- Information Privacy and Security Awareness for Executives Exam (10 minutes)

Security and Privacy Awareness for General Staff (3 hours 1 minute)
Course Code: SAE GEN
This course is designed for general office staff and employees who have access to sensitive information.
- VID 001 Data Privacy in 2 Minutes
- AWA 004 Introduction to Security Awareness (15 minutes)
- AWA 008 Information Privacy - Classifying Data (15 minutes)
- AWA 009 Information Privacy - Protecting Data (15 minutes)
- VID 012 Social Engineering in 2 Minutes
- AWA 018 Social Engineering Awareness (15 minutes)
- VID 010 Physical Security in 2 Minutes
- AWA 017 Physical Security (10 minutes)
- VID 008 PCI Compliance in 2 Minutes
- AWA 015 PCI Compliance (15 minutes)
- JRT 002 SP for Retail Managers (15 minutes)

Security and Privacy Awareness for Retail Managers (1 hour 48 minutes)
Course Code: SAE RM
This course is designed for general office staff and employees who have access to sensitive information.
- VID 001 Data Privacy in 2 Minutes
- AWA 004 Introduction to Security Awareness (15 minutes)
- AWA 008 Information Privacy - Classifying Data (15 minutes)
- AWA 009 Information Privacy - Protecting Data (15 minutes)
- VID 012 Social Engineering in 2 Minutes
- AWA 018 Social Engineering Awareness (15 minutes)
- VID 013 Strong Passwords in 2 Minutes
- AWA 014 Password Security (10 minutes)
- VID 007 Password Security in 2 Minutes
- VID 002 Email Privacy in 2 Minutes
- AWA 010 Email Security (10 minutes)
- VID 009 Phishing in 2 Minutes
- AWA 016 Phishing Awareness (10 minutes)
- VID 005 Malware Prevention in 2 Minutes
- AWA 012 Malware Awareness (10 minutes)
- VID 010 Physical Security in 2 Minutes
- AWA 017 Physical Security (10 minutes)
- JRT 004 SP for Call Center Managers (10 minutes)
- VID 011 Ransomware in 2 Minutes
- VID 008 PCI Compliance in 2 Minutes
- AWA 015 PCI Compliance (15 minutes)

Security and Privacy Awareness for Retail Associates (1 hour 48 minutes)
Course Code: SAE GA
This course is designed for employees who process credit card transactions in person.
- VID 001 Data Privacy in 2 Minutes
- AWA 004 Introduction to Security Awareness (15 minutes)
- AWA 008 Information Privacy - Classifying Data (15 minutes)
- AWA 009 Information Privacy - Protecting Data (15 minutes)
- VID 012 Social Engineering in 2 Minutes
- AWA 018 Social Engineering Awareness (15 minutes)
- VID 010 Physical Security in 2 Minutes
- AWA 017 Physical Security (10 minutes)
- VID 008 PCI Compliance in 2 Minutes
- AWA 015 PCI Compliance (15 minutes)
- JRT 002 SP for Retail Managers (15 minutes)
Security and Privacy Awareness for Call Center Associates (2 hours 40 minutes)
Course Code: SAE CCA
This course is designed for employees who process card-not-present transactions.
• VID 001 Data Privacy in 2 Minutes
• AWA 004 Introduction to Security Awareness (15 minutes)
• AWA 008 Information Privacy - Classifying Data (15 minutes)
• AWA 009 Information Privacy - Protecting Data (15 minutes)
• VID 012 Social Engineering in 2 Minutes
• AWA 018 Social Engineering Awareness (15 minutes)
• VID 013 Strong Passwords in 2 Minutes
• AWA 014 Password Security (10 minutes)
• VID 007 Password Security in 2 Minutes
• VID 002 Email Privacy in 2 Minutes
• AWA 010 Email Security (10 minutes)
• VID 009 Phishing in 2 Minutes
• AWA 016 Phishing Awareness (10 minutes)
• VID 005 Malware Prevention in 2 Minutes
• AWA 012 Malware Awareness (10 minutes)
• VID 010 Physical Security in 2 Minutes
• AWA 017 Physical Security (10 minutes)
• JRT 003 SP for Call Center Associates (15 minutes)
• VID 011 Ransomware in 2 Minutes
• VID 008 PCI Compliance in 2 Minutes
• AWA 015 PCI Compliance (15 minutes)

Security and Privacy Awareness for Compliance Managers (3 hours 4 minutes)
Course Code: SAE PCIP
This course is designed for general or management staff tasked with compliance or risk program management responsibilities.
• VID 001 Data Privacy in 2 Minutes
• AWA 004 Introduction to Security Awareness (15 minutes)
• AWA 008 Information Privacy - Classifying Data (15 minutes)
• AWA 009 Information Privacy - Protecting Data (15 minutes)
• VID 012 Social Engineering in 2 Minutes
• AWA 018 Social Engineering Awareness (15 minutes)
• VID 013 Strong Passwords in 2 Minutes
• AWA 014 Password Security (10 minutes)
• VID 007 Password Security in 2 Minutes
• VID 002 Email Privacy in 2 Minutes
• AWA 010 Email Security (10 minutes)
• VID 009 Phishing in 2 Minutes
• AWA 016 Phishing Awareness (10 minutes)
• VID 005 Malware Prevention in 2 Minutes
• AWA 012 Malware Awareness (10 minutes)
• VID 010 Physical Security in 2 Minutes
• AWA 017 Physical Security (10 minutes)
• VID 006 Mobile Security in 2 Minutes
• AWA 013 Mobile Security (15 minutes)
• VID 008 PCI Compliance in 2 Minutes
• AWA 015 PCI Compliance (15 minutes)
• AWA 002 PCI Business As Usual Compliance (10 minutes)
• VID 011 Ransomware in 2 Minutes
• VID 014 Travel Security in 2 Minutes
• AWA 019 Travel Security (10 minutes)

PCI Fundamentals (1 hour 4 minutes)
Course Code: SAE PCIFUND
This course is designed for general or management staff tasked with compliance or risk program management responsibilities.
• VID 001 Data Privacy in 2 Minutes
• AWA 004 Introduction to Security Awareness (15 minutes)
• AWA 008 Information Privacy - Classifying Data (15 minutes)
• AWA 009 Information Privacy - Protecting Data (15 minutes)
• VID 008 PCI Compliance in 2 Minutes
• AWA 015 PCI Compliance (15 minutes)

General Data Protection Regulation (GDPR) (34 minutes)
Course Code: SAE GDPR
This course is designed for general staff who require a general knowledge of GDPR.
• VID 001 Data Privacy in 2 Minutes
• VID 003 GDPR in 2 Minutes
• AWA 008 Information Privacy - Classifying Data (15 minutes)
• AWA 009 Information Privacy - Protecting Data (15 minutes)
SAE Supplemental Training

Strengthen your security awareness program with videos and posters. Two-minute videos provide introductory or refresher training on privacy and security awareness topics aligned with lesson topics. Posters are available in English, and they are in PDF format. Posters are available for download in the Cybersecurity Education portal and are included with client-hosted content packages.

- VID 001 Data Privacy in 2 Minutes
- VID 002 Email Privacy in 2 Minutes
- VID 003 GDPR in 2 Minutes
- VID 004 IoT in 2 Minutes
- VID 005 Malware Prevention in 2 Minutes
- VID 006 Mobile Security in 2 Minutes
- VID 007 Password Security in 2 Minutes
- VID 008 PCI Compliance in 2 Minutes
- VID 009 Phishing in 2 Minutes
- VID 010 Physical Security in 2 Minutes
- VID 011 Ransomware in 2 Minutes
- VID 012 Social Engineering in 2 Minutes
- VID 013 Strong Passwords in 2 Minutes
- VID 014 Travel Security in 2 Minutes
- VID 015 W-2 Phishing in 2 Minutes
Secure Development Training (SDT)

Trustwave offers a suite of web-based technical courses that introduce your solution development staff to theory and best practices around planning and writing secure code. You can choose to enroll employees in just one of the courses that is most relevant to them, or give them access to an SDT course bundle. No matter what option you select, this section will help you decide which courses are right for your staff.

Secure Development Courses
Use the SDT Courses list to browse our library of SDT courses. Categorized by the stages of the Software Development Life Cycle (SDLC), each course's catalog code, topic, and prerequisites (if any) are listed here to help you decide which topics are most appropriate for your target audience(s). All courses are available in English and content translation is available. The portal is English by default and may be configured in Spanish, French and Portuguese as well as many other languages.

Secure Development Bundles
The Secure Development Bundles shown on page 20 in this document are available to customers using SDT. You can use the Secure Development Bundles page to note which bundles (consisting of various courses) you would like to offer to your staff.
### Security Awareness and Process

These courses cover topics related to fundamental security awareness concepts as they relate to software development.

<table>
<thead>
<tr>
<th>#</th>
<th>Course Name</th>
<th>Course Objectives</th>
<th>Time</th>
<th>Suggested Prerequisites</th>
</tr>
</thead>
</table>
| AWA 101 | Fundamentals of Application Security           | • Learn about the main drivers for application security, fundamental concepts of application security risk management, the anatomy of an application attack, some common attacks, and the concept of input validation as a primary risk mitigation technique.  
• Learn key security principles and best practices for developing secure applications. | 1 hour | Understanding of the Software Development Life Cycle (SDLC) and technologies; basic understanding of software security. |

### Security Engineering

These courses cover topics related to the employment of security awareness strategies as a Software Engineer.

<table>
<thead>
<tr>
<th>#</th>
<th>Course Name</th>
<th>Course Objectives</th>
<th>Time</th>
<th>Suggested Prerequisites</th>
</tr>
</thead>
</table>
| ENG 105 | How to Integrate the Microsoft MS SDL into your SDLC | • Learn the fundamentals of the Microsoft Security Development Lifecycle (SDL) process.  
• Learn about the security requirements for each phase of your SDLC, including Requirements, Design, Implementation, Verification, and Release.  
• Learn about the Agile SDL variation, the Security Development Lifecycle for Line-of-Business Applications (SDL-LOB), and the Microsoft SDL Threat Modeling Tool. | 1 hour | None                                                                                     |
| ENG 205 | Fundamentals of Threat Modeling                | • Learn a question-driven approach to threat modeling that can help you identify security design problems early in the application design process                                                                 | 1 hour | None                                                                                     |
| ENG 211 | How to Create Application Security Design Requirements | • Understand, create, and articulate security requirements.  
• Understand the security engineering process.  
• Recognize key security engineering activities to integrate into the SDLC.  
• Understand software security objectives and apply security design guidelines. | 1 hour | Fundamentals of Application Security (AWA 101)                                            |
| ENG 301 | How to Create an Application Security Threat Model | • Learn to identify the goals of threat modeling and the corresponding Software Development Life Cycle (SDLC) requirements.  
• Identify the roles and responsibilities involved in the threat modeling process.  
• Recognize when and what to threat model.  
• Identify the tools that help with threat modeling.  
• Learn to use the threat modeling process to accurately identify, mitigate and validate threats. | 90 minutes | None                                                                                     |
| ENG 311 | Attack Surface Analysis and Reduction            | • Understand the goals and methodologies of attackers.  
• Identify attack vectors.  
• Learn how to minimize the attack surface of an application.  
• Learn how to define the attack surface of an application.  
• Learn how to reduce the risk to an application by minimizing its attack surfaces. | 1 hour | Fundamentals of Secure Development (COD 101)  
• Architecture Risk Analysis and Remediation (DES 212) |
| ENG 312 | How to Perform a Security Code Review           | • Learn how to organize and prioritize code reviews into segments.  
• Learn how to perform code reviews for the OWASP Top 10 vulnerabilities. | 1 hour | Fundamentals of Secure Development (COD 101)  
• Architecture Risk Analysis and Remediation (DES 212) |
| ENG 391 | Create an Application Security Threat Model for IoT Embedded Systems | • Learn additional information about creating an Application Security threat model.  
• Learn how to map content to specific compliance and regulatory requirements.  
• Learn about key reference resources that support the topics covered in the module.  
• Assess mastery of key concepts. | 30 minutes | How to Create an Application Security Threat Model (ENG 301) |
<table>
<thead>
<tr>
<th>#</th>
<th>Course Name</th>
<th>Course Objectives</th>
<th>Time</th>
<th>Suggested Prerequisites</th>
</tr>
</thead>
</table>
|    | **ENG 392** Attack Surface Analysis and Reduction for IoT Embedded Systems | • Learn additional information about Attack Surface Analysis and Reduction (particularly important to embedded software engineers).  
• Learn about key reference resources that support topics covered in this module.  
• Assess mastery of key concepts.                                                                 | 30 minutes | Attack Surface Analysis and Reduction (ENG 311)                           |
|    | **Secure Design**                                | These courses cover topics related to secure software architecture and design, to help plan security into applications before any code is written. |
|    | **DES 101** Fundamentals of Secure Architecture | • Examine the state of the industry from a security perspective.  
• Learn about the biggest security disasters in software design.  
• Understand that confidentiality, integrity and availability are the three main tenets of information security.  
• Learn how to avoid repeating past information security mistakes.                                                                 | 1 hour | • Fundamentals of Application Security (AWA 101)  
• How to Create Application Security Design Requirements (ENG 211) |
|    | **DES 201** Fundamentals of Cryptography         | • Learn the basic concepts of cryptography and common ways that it is applied, from the perspective of application development.  
• Learn the importance of randomness; the roles of encoding, encryption and hashing; the concepts of symmetric and asymmetric encryption; the purpose of cryptographic keys; and the roles of message authentication codes (MACs) and digital signatures.  
• Learn about complexity of cryptography.                                                                 | 2 hours| • Fundamentals of Application Security (AWA 101)  
• Fundamentals of Secure Development (COD 101)  
• OWASP Top Ten Threats and Mitigations (DES 221) |
<p>|    | <strong>DES 212</strong> Architecture Risk Analysis and Remediation | • Learn concepts, methods and techniques for analyzing the architecture and design of a software system for security flaws.                                                                 | 1 hour | Fundamentals of Application Security (AWA 101)                           |
|    | <strong>DES 214</strong> Securing Network Access             | • Learn about how Network Access Control can be used to secure systems on a network.                                                                 | 30 minutes | This course is part of the Secure Enterprise Infrastructure Series        |
|    | <strong>DES 215</strong> Securing Operating Systems          | • Learn about common operating system threats and how to best mitigate those threats.                                                                | 30 minutes | This course is part of the Secure Enterprise Infrastructure Series        |
|    | <strong>DES 216</strong> Securing Cloud Instances           | • Learn about the top threats to Cloud resources and how to mitigate them using application security best practices.                                    | 30 minutes | This course is part of the Secure Enterprise Infrastructure Series        |
|    | <strong>DES 217</strong> Application, Technical and Physical Access Controls | • Learn about the risks associated with data breaches and how to implement strong access controls and security policies that protect applications, systems and sensitive data. | 30 minutes | This course is part of the Secure Enterprise Infrastructure Series        |
|    | <strong>DES 222</strong> Mitigating Injection                | • Learn how to mitigate the risks associated with injection.                                                                                         | 12 minutes | This course is part of the OWASP 2017 Series                             |
|    | <strong>DES 223</strong> Mitigating Broken Authentication    | • Learn how to mitigate the risks associated with broken authentication.                                                                              | 12 minutes | This course is part of the OWASP 2017 Series                             |
|    | <strong>DES 224</strong> Mitigating Sensitive Data Exposure  | • Learn how to mitigate the risks associated with sensitive data exposure.                                                                             | 12 minutes | This course is part of the OWASP 2017 Series                             |
|    | <strong>DES 225</strong> Mitigating XML External Entities (XXE) | • Learn how to mitigate the risks associated with XML External Entities (XXE).                                                                          | 12 minutes | This course is part of the OWASP 2017 Series                             |
|    | <strong>DES 226</strong> Mitigating Broken Access Control (12) | • Learn how to mitigate the risks associated with broken access control.                                                                 | 12 minutes | This course is part of the OWASP 2017 Series                             |
|    | <strong>DES 227</strong> Mitigating Security Misconfiguration | • Learn how to mitigate the risks associated with security misconfiguration.                                                                           | 12 minutes | This course is part of the OWASP 2017 Series                             |</p>
<table>
<thead>
<tr>
<th>#</th>
<th>Course Name</th>
<th>Course Objectives</th>
<th>Time</th>
<th>Suggested Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES 228</td>
<td>Mitigating Cross Site Scripting (XSS)</td>
<td>• Learn how to mitigate the risks associated with Cross-Site Scripting (XSS).</td>
<td>12 minutes</td>
<td>This course is part of the OWASP 2017 Series</td>
</tr>
<tr>
<td>DES 229</td>
<td>Mitigating Insecure Deserialization</td>
<td>• Learn how to mitigate the risks associated with insecure deserialization.</td>
<td>12 minutes</td>
<td>This course is part of the OWASP 2017 Series</td>
</tr>
<tr>
<td>DES 230</td>
<td>Mitigating Use of Components with Known Vulnerabilities</td>
<td>• Learn how to mitigate the risks associated with using components with known vulnerabilities.</td>
<td>12 minutes</td>
<td>This course is part of the OWASP 2017 Series</td>
</tr>
<tr>
<td>DES 231</td>
<td>Mitigating Insufficient Logging &amp; Monitoring Vulnerabilities</td>
<td>• Learn how to mitigate the risks associated with insufficient logging and monitoring.</td>
<td>12 minutes</td>
<td>This course is part of the OWASP 2017 Series</td>
</tr>
<tr>
<td>DES 292</td>
<td>Architecture Risk Analysis and Remediation for IoT Embedded Systems</td>
<td>• Learn additional information about Architecture Risk Analysis and Remediation training (of particular importance to embedded software engineers).</td>
<td>30 minutes</td>
<td>Architecture Risk Analysis &amp; Remediation (DES 212)</td>
</tr>
<tr>
<td>DES 311</td>
<td>Creating Secure Application Architecture</td>
<td>• Learn how to harden applications and make them more difficult for intruders to breach. • Learn about compartmentalization, centralized input, and data validation as methods to protect applications from malicious input.</td>
<td>2 hours</td>
<td>None</td>
</tr>
<tr>
<td>DES 352</td>
<td>Creating Secure Over the Air (OTA) Automotive System Updates</td>
<td>• Learn about secure design considerations for over-the-air (OTA) updates for automotive systems. • After completing this course, you will be able to identify the benefits and risks of OTA automotive system updates, understand the importance of public key cryptography to the security of these updates, and identify secure design considerations for development, delivery, and installation of OTA automotive system updates.</td>
<td>90 minutes</td>
<td>• Fundamentals of Secure Mobile Development (COD 110) • IoT Embedded Systems Security - Fundamentals of Secure Embedded Software Development (COD 160)</td>
</tr>
<tr>
<td>DES 391</td>
<td>Creating Secure Application Architecture for IoT Embedded Systems</td>
<td>• Learn additional information about Creating Secure Application Architecture (of particular importance to embedded software engineers). • Assess mastery of key concepts.</td>
<td>30 minutes</td>
<td>Creating Secure Application Architecture (DES 311)</td>
</tr>
</tbody>
</table>

**Secure Coding** These courses cover topics related to the implementation stage of the Software Development Life Cycle (when code is actually written).

<table>
<thead>
<tr>
<th>#</th>
<th>Course Name</th>
<th>Course Objectives</th>
<th>Time</th>
<th>Suggested Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>COD 101</td>
<td>Fundamentals of Secure Development</td>
<td>• Learn about the need for secure software development. • Learn about the models, standards, and guidelines you can use to understand security issues and improve the security posture of your applications. • Learn about key application security principles. • Learn how to integrate secure development practices into the SDLC.</td>
<td>80 minutes</td>
<td>None</td>
</tr>
<tr>
<td>COD 110</td>
<td>Fundamentals of Secure Mobile Development</td>
<td>• Learn about common risks associated with mobile applications. • Learn mobile application development best practices. • Understand mobile development threats and risks.</td>
<td>2 hours</td>
<td>None</td>
</tr>
<tr>
<td>COD 141</td>
<td>Fundamentals of Secure Database Development</td>
<td>• Understand database development best practices.</td>
<td>1 hour 50 minutes</td>
<td>Fundamentals of Application Security (AWA 101)</td>
</tr>
<tr>
<td>#</td>
<td>Course Name</td>
<td>Course Objectives</td>
<td>Time</td>
<td>Suggested Prerequisites</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>COD 152</td>
<td>Fundamentals of Secure Cloud Development</td>
<td>• Recognize the common risks associated with Cloud applications, including the security features of the different series models (IaaS, PaaS and SaaS).&lt;br&gt;• Learn how to identify and mitigate the most common vulnerabilities and the unique security challenges of “Big Data”.&lt;br&gt;• Learn how to apply the Microsoft SDL to cloud applications.</td>
<td>30 minutes</td>
<td>None</td>
</tr>
<tr>
<td>COD 153</td>
<td>Fundamentals of Secure AJAX Code</td>
<td>• Learn about AJAX technology and its common vulnerabilities and attack vectors.&lt;br&gt;• Identify the differences between regular and AJAX applications, common AJAX vulnerabilities that attackers tend to exploit, and major threats to AJAX applications.</td>
<td>35 minutes</td>
<td>None</td>
</tr>
<tr>
<td>COD 160</td>
<td>Fundamentals of Secure Embedded Software Development</td>
<td>• Learn about security issues inherent to embedded device architecture.&lt;br&gt;• Learn about techniques to identify system security and performance requirements, develop appropriate security architecture, select the correct mitigations, and develop policies that can ensure the secure operation of your system.</td>
<td>90 minutes</td>
<td>None</td>
</tr>
<tr>
<td>COD 170</td>
<td>Identifying Threats to Mainframe COBOL Applications and Data</td>
<td>• Learn about common security issues that affect the confidentiality, integrity and availability of COBOL programs or mainframes.</td>
<td>20 minutes</td>
<td>None</td>
</tr>
<tr>
<td>COD 190</td>
<td>IoT Embedded Systems Security - Fundamentals of Secure Mobile Development</td>
<td>• Learn additional information about Secure Mobile Development (of particular importance to embedded software engineers).&lt;br&gt;• Assess mastery of key concepts.</td>
<td>30 minutes</td>
<td>Fundamentals of Secure Mobile Development (COD 110)</td>
</tr>
<tr>
<td>COD 211</td>
<td>Creating Secure Code – Java Foundations</td>
<td>• Learn best practices and techniques for secure application development in Java.</td>
<td>2.5 hours</td>
<td>• Fundamentals of Application Security (AWA 101)&lt;br&gt;• Fundamentals of Secure Development (COD 101)&lt;br&gt;• OWASP Top 10 - Threats and Mitigations (DES 221)</td>
</tr>
<tr>
<td>COD 212</td>
<td>Creating Secure Code – C/C++ Foundations</td>
<td>• Learn best practices and techniques for secure application development in C/C++.</td>
<td>2 hours</td>
<td>• Fundamentals of Application Security (AWA 101)&lt;br&gt;• Fundamentals of Secure Development (COD 101)&lt;br&gt;• OWASP Top 10 - Threats and Mitigations (DES 221)</td>
</tr>
<tr>
<td>COD 215</td>
<td>Creating Secure Code – .NET Framework Foundations</td>
<td>• Learn about .NET 4 security features.&lt;br&gt;• Learn about changes in .NET 4.&lt;br&gt;• Learn secure coding best practices.</td>
<td>2 hours</td>
<td>Fundamentals of Secure Development (COD 101)</td>
</tr>
<tr>
<td>COD 219</td>
<td>Creating Secure Code - SAP ABAP Foundations</td>
<td>• Learn best practices and techniques for secure SAP application development using Java and ABAP.&lt;br&gt;• Learn about basic application security principles, input validation in SAP applications, common application security vulnerabilities and mitigations, protecting data using encryption, and conducting security code analysis and code reviews.</td>
<td>90 minutes</td>
<td>• Fundamentals of Secure Development (COD 101)&lt;br&gt;• Fundamentals of Application Security (AWA 101)&lt;br&gt;• OWASP Top 10 - Threats and Mitigations (DES 221)</td>
</tr>
<tr>
<td>COD 222</td>
<td>PCI DSS v3.2 Best Practices for Developers</td>
<td>• Learn about PCI DSS best practices and how to use them to address application security issues.</td>
<td>1 hour</td>
<td>Fundamentals of Secure Architecture (DES 101)</td>
</tr>
<tr>
<td>COD 225</td>
<td>Insecure IoT Web Interface</td>
<td>• Learn how to identify common threats to IoT web interfaces and apply best practices to mitigate these threats.</td>
<td>10 minutes</td>
<td>This course is part of the IoT Specialization Series</td>
</tr>
<tr>
<td>#</td>
<td>Course Name</td>
<td>Course Objectives</td>
<td>Time</td>
<td>Suggested Prerequisites</td>
</tr>
<tr>
<td>----</td>
<td>-------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>---------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>COD 226</td>
<td>Insufficient IoT Authentication/Authorization</td>
<td>• Learn how to implement secure authentication and authorization for IoT devices.</td>
<td>10 minutes</td>
<td>This course is part of the IoT Specialization Series</td>
</tr>
<tr>
<td>COD 227</td>
<td>Insecure IoT Network Devices</td>
<td>• Learn about the vulnerabilities of insecure network devices within the context of IoT devices and best practices to protect network services on IoT devices.</td>
<td>10 minutes</td>
<td>This course is part of the IoT Specialization Series</td>
</tr>
<tr>
<td>COD 228</td>
<td>Insecure IoT Communications</td>
<td>• Learn about the risks of insecure communications.</td>
<td>10 minutes</td>
<td>This course is part of the IoT Specialization Series</td>
</tr>
<tr>
<td>COD 229</td>
<td>Insecure IoT Mobile Interface</td>
<td>• Learn about best practices for protecting mobile applications used for IoT solutions.</td>
<td>10 minutes</td>
<td>This course is part of the IoT Specialization Series</td>
</tr>
<tr>
<td>COD 230</td>
<td>Insecure Software/Firmware</td>
<td>• Learn how to securely distribute updates that fix known vulnerabilities in software or firmware for your IoT devices.</td>
<td>10 minutes</td>
<td>This course is part of the IoT Specialization Series</td>
</tr>
<tr>
<td>COD 234</td>
<td>Mobile Threats and Mitigations</td>
<td>• Learn about best practices for identifying and mitigating the most common threats to mobile applications and their data.</td>
<td>20 minutes</td>
<td>This course is part of the OWASP Mobile Series</td>
</tr>
<tr>
<td>COD 235</td>
<td>Defending Mobile Data with Cryptography</td>
<td>• Learn about best practices for implementing strong cryptography to protect mobile applications and their data.</td>
<td>20 minutes</td>
<td>This course is part of the OWASP Mobile Series</td>
</tr>
<tr>
<td>COD 236</td>
<td>Mobile App Authentication and Authorization</td>
<td>• Learn how to integrate secure authentication and authorization into your mobile application.</td>
<td>20 minutes</td>
<td>This course is part of the OWASP Mobile Series</td>
</tr>
<tr>
<td>COD 237</td>
<td>Defending Mobile App Code</td>
<td>• Learn how to integrate secure authentication and authorization into your mobile application.</td>
<td>20 minutes</td>
<td>This course is part of the OWASP Mobile Series</td>
</tr>
<tr>
<td>COD 242</td>
<td>Creating Secure SQL Applications</td>
<td>• Learn how to protect sensitive data while ensuring the integrity of applications running on the Microsoft SQL Server Engine and Azure SQL Database.</td>
<td>40 minutes</td>
<td>n Series</td>
</tr>
</tbody>
</table>
| COD 251 | Creating Secure AJAX Code - ASP.NET Foundations | • Understand how to mitigate common vulnerabilities and protect against common attack vectors.  
• Identify threats to AJAX applications from cross-site scripting and other attacks.  
• Learn how to implement countermeasures against attacks. | 35 minutes | Fundamentals of Secure AJAX Code (COD 153)                   |
| COD 252 | Creating Secure AJAX Code – Java Foundations | • Understand how to mitigate common vulnerabilities and protect against common attack vectors.  
• Identify threats to AJAX applications from cross-site scripting and other attacks.  
• Learn how to implement countermeasures against attacks. | 35 minutes | Fundamentals of Secure AJAX Code (COD 153)                   |
| COD 253 | Creating Secure AWS Cloud Applications     | • Learn about security vulnerabilities, threats and mitigations for Amazon Web Services (AWS) cloud computing services.  
• Learn about Elastic Compute Cloud (EC2), Virtual Private Cloud (VPC), and four additional core AWS: Identity and Access Management (IAM), DynamoDB Flat Database Service, Relational Database Service (RDS), and Simple Storage Service (S3).  
• Learn about ancillary AWS.  
• After completing this course, you will be able to identify the most common security threats to cloud development and best practices to protect against these threats. You will also be able to identify AWS security features and ways to integrate them into your AWS resources. | 1 hour   | None                                                        |
<table>
<thead>
<tr>
<th>#</th>
<th>Course Name</th>
<th>Course Objectives</th>
<th>Time</th>
<th>Suggested Prerequisites</th>
</tr>
</thead>
</table>
| COD 254 | Creating Secure Azure Applications            | • Learn about the risks associated with creating and deploying applications on Microsoft’s Azure cloud platform.  
• Recognize core security considerations for Azure Virtual Machine (VM) security, authentication and access control, legacy .Net Framework applications, Azure web sites and the Microsoft WebMatrix3 IDE. | 90 minutes | None                                                                                   |
| COD 255 | Creating Secure Code - Web API Foundations   | • Learn about common web services that may put your application at risk.  
• Learn best practices that you should incorporate to mitigate the risk from web services attacks.  
• Understand various web services threats and the cause and impact of web services attacks.  
• Learn how to implement secure development best practices to protect web services. | 2 hours  | • Fundamentals of Application Security (AWA 101)  
• Fundamentals of Secure Development (COD 101)  
• OWASP Top 10 Threats and Mitigations (DES 221) |
| COD 256 | Creating Secure Code - Ruby on Rails Foundations | • Learn best practices and techniques for secure application development with Ruby on Rails.  
• Learn to identify and mitigate injection vulnerabilities, such as SQL injection and cross-site scripting.  
• Learn how to build strong session management into your Rails applications and prevent other common vulnerabilities, such as cross-site request forgery and direct object access. | 90 minutes | Fundamentals of Application Security (AWA 101) |
| COD 257 | Creating Secure Python Web Applications      | • Learn about best practices and techniques for secure application development with Python.  
• Understand various types of injection vulnerabilities.  
• Understand how to build strong session management into your Python web application and how to prevent common vulnerabilities.  
• Recognize file system threats to web applications, including vulnerabilities with path traversal, temporary files, and insecure client redirects. | 45 minutes | None                                                                                   |
| COD 261 | Threats to Scripts                            | • Learn about the impact of incorrect script development or lax security measures.  
• Learn about the most common scripting vulnerabilities, including cached secrets, a variety of injection vulnerabilities, weaknesses related to permissions and privileges, and the threat of resource exhaustion. | 30 minutes | This course is part of the Secure Scripting Series                                       |
<p>| COD 262 | Fundamentals of Secure Scripting             | • Learn how shell scripting languages compare with more modern interpreted languages; several information security principles including least privilege and defense in depth; the importance of data validation; and operating system portability issues. | 30 minutes | This course is part of the Secure Scripting Series                                       |
| COD 263 | Secure Scripting with Perl, Python, Bash and Ruby | • Learn about the importance of error and exception handling in shell scripts and interpreted languages, common syntax pitfalls, and how to prevent or mitigate several common vulnerabilities. | 30 minutes | This course is part of the Secure Scripting Series                                      |
| COD 264 | Protecting Sensitive Data while Scripting    | • Learn how to use filesystem operations safely to protect files; system hardening; cryptography basics; and the importance of up-to-date communication security techniques. | 30 minutes | This course is part of the Secure Scripting Series                                      |
| COD 270 | Creating Secure COBOL and Mainframe Applications | • Learn about countermeasures for security vulnerabilities on the mainframe, such as input validation, parameterized APIs, strong cryptography, and being aware of memory management issues. | 25 minutes | None                                                                                   |</p>
<table>
<thead>
<tr>
<th>#</th>
<th>Course Name</th>
<th>Course Objectives</th>
<th>Time</th>
<th>Suggested Prerequisites</th>
</tr>
</thead>
</table>
| COD 311| Creating Secure Code ASP.NET MVC Applications | • Learn about ASP .NET and Web API code security issues that affect MVC and Web API applications.  
• Learn methods to protect your application from attacks against MVC’s model-binding behavior.  
• Learn methods to protect your application from cross-site scripting, cross-site request forgery and malicious URL redirects.  
• Learn about the Web API pipeline and how to implement authentication and authorization in Web API applications. | 2 hours         | • Fundamentals of Application Security (AWA 101)  
• Fundamentals of Secure Development (COD 101)  
• OWASP Top 10 – Threats and Mitigations (DES 221)  
| COD 312| Creating Secure C/C++ Code                      | • Learn techniques for securing your C/C++ applications.  
• Learn about secure memory management in C/C++, protecting and authenticating sensitive data with symmetric and public key cryptography, and secure communications with TLS. | 2 hours         | • Fundamentals of Secure Development (COD 101)  
• Fundamentals of Application Security (AWA 101)  
• OWASP Top 10 – Threats and Mitigations (DES 221)  
• Creating Secure Code – C/C++ Foundations (COD 212) |
| COD 313| Creating Secure Java Code                       | • Identify and use the components of the Java security model.  
• Identify how to use JAAS to control user authentication and authorization in your Java application.  
• Learn how to implement cryptography to sign and verify Java jar files. | 35 minutes      | • Fundamentals of Application Security (AWA 101)  
• Fundamentals of Secure Development (COD 101)  
• OWASP Top 10 – Threats and Mitigations (DES 221)  
• Creating Secure Code – Java Foundations (COD 211) |
| COD 314| Creating Secure C# Code                         | • Learn about common security vulnerabilities that can be mitigated by proper input validation, other common security vulnerabilities and their mitigations, secure error handling and logging, and secure communication.  
• Learn about the unique features of C# and the .NET framework that help protect against security vulnerabilities. | 2 hours and 30 minutes | • Fundamentals of Application Security (AWA 101)  
• Fundamentals of Secure Development (COD 101)  
• OWASP Top 10 – Threats and Mitigations (DES 221) |
| COD 315| Creating Secure PHP Code                        | • Learn the security principles for building secure PHP applications.  
• Assess mastery of key concepts. | 2 hours         | • Fundamentals of Application Security (AWA 101)  
• Fundamentals of Secure Development (COD 101) |
| COD 317| Creating Secure iOS Code in Swift               | • Recognize common iOS application vulnerabilities and learn secure coding best practices.  
• Recognize and mitigate threats by leveraging iOS and Swift security services while also implementing secure coding best practices. | 90 minutes      | None |
| COD 318| Creating Secure Android Code in Java            | • Learn about common Android application vulnerabilities.  
• Learn secure coding best practices using Java and the Android Software Development Kit (SDK).  
• Identify and mitigate a variety of attacks. | 90 minutes      | None |
| COD 351| Creating Secure HTML5 Code                      | • Learn about the development of secure HTML5 code.  
• Learn about common HTML5 application vulnerabilities and threats, and secure coding best practices.  
• Upon completion of this class, participants will be able to identify ways in which the expanded attack surface introduced with HTML5 might impact your web applications.  
• Participants will also be able to identify new security features available with HTML5, as well as countermeasures and best practices to mitigate the application’s exposure to attack. | 80 minutes      | None |
<table>
<thead>
<tr>
<th>#</th>
<th>Course Name</th>
<th>Course Objectives</th>
<th>Time</th>
<th>Suggested Prerequisites</th>
</tr>
</thead>
</table>
| COD | Creating Secure jQuery Code                    | • Learn about common client-side vulnerabilities and threats to jQuery applications, and techniques for mitigating these vulnerabilities and threats.  
• Learn about how to implement new HTML5 security features to secure jQuery applications, and best practices to secure local storage and implement transport layer security.  
• Be able to describe the threats that can impact your jQuery code and describe the countermeasures to address these threats.                                                                                                                                                                                                                                                                                                                                                   | 90 minutes | None                                                                                                        |
| TST | Fundamentals of Security Testing                | • Learn security testing concepts and processes.  
• Learn how to conduct effective security testing.  
• Identify common security issues during testing to uncover security vulnerabilities.                                                                                                                                                                                                                                                                                                                                                                                                          | 2 hours  | Fundamentals of Application Security (AWA 101)  
How to Create Application Security Design Requirements (ENG 211)                                                                                                      |
| TST | Fundamentals of Security Testing for IoT        | • Learn additional information about the Fundamentals of Security Testing training (of particular importance to embedded software engineers).  
• Assess mastery of key concepts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 30 minutes | Fundamentals of Security Testing (TST 101)                                                                 |
| TST | Testing for CWE SANS Top 25 Software Errors      | • Identify and mitigate each of the CWE’s 25 most dangerous software errors.  
• Learn techniques for spotting common security issues through code review and testing.  
• Identify common security defects and their potential impact to your application.  
• Identify specific types of security vulnerabilities associated with different technologies.                                                                                                                                                                                                                                                                                                                                                              | 3 hours  | Fundamentals of Application Security (AWA 101)                                                                 |
| TST | How to Test for the OWASP Top 10               | • Learn about the top ten OWASP flaws and how to perform testing to identify these flaws in web applications.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 1 hour and 30 minutes | Fundamentals of Security Testing (TST 101)                                                                 |
| TST | Classes of Security Defects - IoT Embedded      | • Learn additional information about Security Defects Classes (of particular importance to embedded software engineers).  
• Assess mastery of key concepts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 30 minutes | Classes of Security Defects (TST 201)                                                                    |
| TST | Advanced Software Security Testing - Tools and   | • Learn about testing for specific security weaknesses.  
• Learn about the top ten types of attacks and the tools to use to test for these attacks.  
• Learn how to test software applications for susceptibility to the top ten attacks.                                                                                                                                                                                                                                                                                                                                                                                                   | 2 hours  | Fundamentals of Security Testing (TST 101)  
Classes of Security Defects (TST 201)                                                                                                                                       |
| TST | Exploiting Buffer Overflows                    | • Understand and mitigate buffer-overflow exploits.  
• Understand the challenges faced by exploit code and how different exploitation techniques overcome environmental limitations.                                                                                                                                                                                                                                                                                                                                                                               | 2 hours  | Creating Secure C/C++ Code (COD 312)                                                                    |
| TST | IoT Advanced Embedded Software Security Testing | • Learn additional information about Software Security Testing (of particular importance to embedded software engineers).  
• Assess mastery of key concepts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 30 minutes | Advanced Software Security Testing – Tools & Techniques (TST 401)                                       |
Secure Development Training Bundles

Use this section to determine which bundles you want to provide for your staff. Descriptions of the courses in each bundle can be found in the SDT Courses List. Custom bundles, consisting of up to five courses, can be set up by request.

Contact your Trustwave account manager if you would like to configure a custom bundle or add advanced training courses.

C/C++ Developer
- AWA 101 Fundamentals of Application Security
- COD 101 Fundamentals of Secure Development
- COD 160 Fundamentals of Secure Embedded Development
- DES 201 Fundamentals of Cryptography
- COD 212 Creating Secure Code - C/C++ Foundations

C/C++ Developer II
- COD 312 Creating Secure C/C++ Code
- ENG 301 How to Create an Application Security Threat Model
- ENG 312 How to Perform a Security Code Review

Database Developer
- AWA 101 Fundamentals of Application Security
- COD 141 Fundamentals of Secure Database Development
- DES 201 Fundamentals of Cryptography
- ENG 301 How to Create an Application Security Threat Model
- ENG 312 How to Perform a Security Code Review

Java Developer
- AWA 101 Fundamentals of Application Security
- COD 101 Fundamentals of Secure Development
- COD 211 Creating Secure Code - Java Foundations
- COD 252 Creating Secure AJAX Code - Java Foundations

Java Developer II
- COD 313 Creating Secure Java Code
- COD 352 Creating Secure jQuery Code
- ENG 301 How to Create an Application Security Threat Model
- ENG 312 How to Perform a Security Code Review
- COD 351 Creating Secure HTML5 Code

Mobile Developer
- AWA 101 Fundamentals of Application Security
- COD 110 Fundamentals of Secure Mobile Development
- COD 317 Creating Secure iOS Code in Swift
- COD 318 Creating Secure Android Code in Java

PCI Developer
- AWA 101 Fundamentals of Application Security
- COD 222 PCI DSS v 3.2 Best Practices for Developers
- DES 221 OWASP Top 10 - Threats and Mitigations
- ENG 301 How to Create an Application Security Threat Model
- ENG 312 How to Perform a Security Code Review

PHP Developer
- AWA 101 Fundamentals of Application Security
- COD 153 Fundamentals of Secure AJAX Code
- COD 315 Creating Secure PHP Code

Project Manager
- AWA 101 Fundamentals of Application Security
- COD 311 Creating Secure Code ASP.NET MVC Applications
- DES 101 Fundamentals of Secure Architecture
- ENG 211 How to Create Application Security Design Requirements

Software Architect
- AWA 101 Fundamentals of Application Security
- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation

Test/QA (Embedded QA also available)
- TST 101 Fundamentals of Security Testing
- TST 201 Testing for CWE SANS Top 25 Software Errors
- TST 211 How to Test for the OWASP Top 10
- ENG 312 How to Perform a Security Code Review
- TST 401 Advanced Software Security Testing - Tools & Techniques

.NET Developer
- AWA 101 Fundamentals of Application Security
- COD 251 Creating Secure AJAX Code - ASP.NET Foundations
- COD 311 Creating Secure Code ASPNET MVC Applications

Cloud Developer
- AWA 101 Fundamentals of Application Security
- DES 201 Fundamentals of Cryptography
- COD 253 Creating Secure AWS Cloud Applications
- COD 254 CreatingSecure Azure Applications

Embedded Developer
- AWA 101 Fundamentals of Application Security
- DES 201 Fundamentals of Cryptography
- COD 160 Fundamentals of Secure Embedded Software Development
- COD 212 Creating Secure Code - C/C++ Foundations
Embedded Architect

- DES 101 Fundamentals of Secure Architecture
- COD 110 Fundamentals of Secure Mobile Development
- DES 201 Fundamentals of Cryptography
- DES 212 Architecture Risk Analysis and Remediation
- DES 292 Architecture Risk Analysis and Remediation for Embedded Systems

Embedded QA

- TST 101 Fundamentals of Security Testing
- TST 191 Fundamentals of Security Testing for IoT Embedded Systems
- TST 201 Testing for CWE SANS Top 25 Software Errors
- TST 291 Classes of Security Defects - IoT Embedded Systems
- ENG 312 How to Perform a Security Code Review

IT Architect

- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- ENG 211 How to Create Application Security Design Requirements
- ENG 301 How to Create an Application Security Threat Model

Systems Leadership

- COD 101 Fundamentals of Secure Development
- DES 311 Creating Secure Application Architecture

Internet of Things (IoT) Developer

- COD 225 Insecure IoT Web Interfaces
- COD 226 Insecure IoT Authentication and Authorization
- COD 227 Insecure IoT Network Services
- COD 228 Insecure IoT Communications
- COD 229 Insecure IoT Mobile Interface