ESCRYPT security trainings and coachings

Empowering Tomorrow's Automotive Software
www.etas.com

ETAS

Learn and understand automotive security

ETAS cybersecurity experts have long since stopped teaching only the basics of cryptography. Instead, we channel our years of experience in embedded security, gained during numerous industry projects, to provide practical examples and the latest technological developments.

Our training course portfolio imparts a solid understanding of security for embedded devices, thereby laying the foundation for the development of secure technologies.

Your advantages

- We have more than 15 years of experience in automotive security
- Our trainings are based on numerous customer projects and include up-to-date-knowledge about the industry and its development
- All our trainers have a background in IT security and years of practical experience with insights from various customer projects
- Upon completion, each participant receives a certificate of attendance

Designed to suit your needs

- Wide range of topics that cover theoretical as well as practical aspects
- Including discussions, real-world examples as well as best practice solutions
- Offered worldwide and when possible in local language
- In-house trainings at your location, in one of our offices as well as online sessions
- Individual training concepts on request
- Recommended group sizes from 8 to 12 participants

Trainings

Onboard – Automotive security

	Training	Description	Duration
Basic	**Secure product design**	Fundamentals of information security including technical and organizational aspects for product development.	2 days
	Security testing	Introduction to security testing methods for the entire lifecycle.	1 day
Advanced	**Secure connected products**	Advanced security aspects of connected products explaining best practices to secure communication.	1 day
	Automotive security	A holistic view on automotive security with best-practices for hardware and software in modern automotive systems.	2 days

Technology and technical standard security trainings

	Training	Description	Duration
Basic	**AUTOSAR security**	Overview about the general security architecture and the dedicated security building blocks offered by Classic and Adaptive AUTOSAR.	1 day
	Information Security Standards and Requirements Catalogs	This training gives an overall understanding of information security systems and standards, and how they translate into technology standards and best practices.	1 day
	Windows security	Learn about common attacks on Windows installations and explore tools like Command & Control frameworks and malware like Mimikatz that attackers might also use in the wild.	1 day
Advanced	**ISO/SAE 21434 security engineering and management**	Introduction to ISO/SAE 21434 cybersecurity management and engineering activities for the entire lifecycle in context of UNECE R155.	2 days

Offboard – Enterprise security trainings and coaching programs

	Training	Description	Duration
Basic	**Web application security**	Introduction to web application security including a hands-on hacking lab for participants.	1 day
Coaching	**Security risk analysis**	Why, when, and how to perform a security risk analysis. We support you to create a security risk analysis for one of your own systems.	3 days
	Security testing strategy	Develop a strategy how to approach security testing for your organization and products.	1 day
	Threat modeling	Learn how to do a threat model for enterprise systems following international used standards.	2 days

Onboard – Automotive security trainings

Basic training: Secure product design

Training topics

- Get to know different aspects of security (e.g., theory vs. practice, challenges)
- Learn and understand security basics (e.g., basic terminology)
- Find out how to set up a secure software development lifecycle
- Establish fundamental knowledge about cryptographic tools, algorithms, and protocols
- Understand important aspects of access control (authentication and authorization)
- Learn to apply main security principles
- Secure coding module option: comprehend secure coding techniques
- Risk analysis module option: learn how to apply a risk-based approach towards security (e.g., economic security)

Target group

- Product managers and project managers who need to establish a solid understanding about general security principles, processes and tools that are necessary for secure product design
- System engineers and system architects who are responsible for developing and analyzing security requirements and for defining security concepts

Requirements

- Basic technical understanding of mathematical and information technology on engineering level
- No security background is necessary

Duration:
2 days / 16 hours

Languages:
German / English / Chinese / Japanese / Korean

Location:
- ETAS site
- customer site
- conference hotel
- online

Day 1

Security basics
- Discussion of recent IT security threats
- Different aspects of IT security
- Basic terminology
- Generic security framework

Secure software development
- Economic security
- Security activities for a software development process
- Conventional software development
- Agile software development

Cryptographic primitives
- Benefits and limitations of cryptography
- Fundamental cryptographic principles
- Symmetric and asymmetric tools & algorithms
- Cryptographic protocols
- Application & practical advices

Day 2

Access control: authentication
- Password-based authentication & secure password management
- Multi-factor authentication
- Implementation aspects

Access control: authorization
- Permission management & access control lists, role-based access control
- Capabilities & secure session management

Security principles & concepts
- Security principles (defense in depth, keep it simple, least privilege)
- Security concepts (trust boundaries, separation of duties, error & exception handling)

Secure coding
- Secure coding in the development process
- Weaknesses, vulnerabilities & attack references
- Best practices in defensive coding & secure coding guidelines

Onboard – Automotive security trainings

Basic training: Security testing

Training topics

- Get to know the motivation, challenges and limitations of security testing
- Find out how to thoroughly consider security testing in the product development lifecycle (e.g., testing activities in the different phases of the lifecycle)
- Get an overview of different security testing methods and understand the differences
- Learn and understand the basic principles of security testing
- Learn and understand "what" to target in the security testing in which testing setup (e.g., systems, devices, components, interfaces)
- Get to know how to handle identified weaknesses and which mitigation options exist
- Understand the requirements for security testing from the most prominent standards and regulations
- Interactive exercises to strengthen understanding of individual topics

Target group

- Product managers, project managers, test managers, and security managers who need to establish a solid understanding about security testing methods and how to apply them throughout the development lifecycle.
- System engineers, system architects and testers who are responsible for the execution of test strategies

Requirements

- Technical understanding of systems/products and system/product development
- Basic understanding of IT security is helpful

Duration:
1 day / 8 hours

Languages:
German / English

Location:
- ETAS site
- customer site
- conference hotel
- online

Day 1

Introduction

- Why is practical security testing important? – Real-World Example
- Security Testing in UNECE WP.29 and ISO/SAE DIS 21434*

When to test in the product development lifecycle

- Introduction of a general testing lifecycle form the start in the "analysis phase" until the end in the "phase-out"
- Recommendation of security testing activities for each lifecycle phase
- Considering continuous integrated security testing during development

Security testing methods and principles

- Blackbox vs. greybox vs. whitebox testing
- Security testing methods:
  - Penetration testing, Vulnerability scanning, Functional security testing, Code analysis, Fuzzing, Hardware / side channel attack testing
- General security testing principles

What to test in the automotive environment

- Overview of security relevant entities, systems, protocols, components, etc. in the automotive vehicle and surrounding environment
- Potential attack points and paths in a modern connected vehicle
- Different testing scopes and testing setups with advantages and disadvantages
- Different aspects of system, device, component and network testing
- How to handle 3rd party components in security testing

Handling of findings and testing resources

- Process for the handling of findings with mitigation options
- Security testing resources with their challenges and competence requirements

Example pentest report and evaluation methodologies

- Important aspects of a security test report
- Investigation of an example test report with example findings and ratings
- Discussion on different rating methodologies: CVSS, ETAS proprietary rating, ECVSS

* Content tailored for automotive customers is optional

Advanced training: Secure connected products

Training topics

- Understand distinct security aspects regarding connectivity
- Get to know important aspects of advanced access control
- Establish an overview knowledge of secure protocol configurations and pitfalls
- Learn the basics about protocols for the internet of things
- Comprehend the threats to interfaces and how to alleviate them
- Find out the basics about web services and possible vulnerabilities

Target group

- Product or project managers who need to establish a solid understanding how secure products are properly secured
- Product engineers who are responsible for analyzing and defining security requirements and for defining security concepts

Requirements

- Basic technical understanding of mathematical and information technology (engineering level)
- Basic technical understanding of cryptography and IT security (i.e., knowledge from secure product design or equivalent)

Duration:
1 day / 8 hours

Languages:
German / English

Location:
- ETAS site
- customer site
- conference hotel
- online

Day 1

Connectivity basics
- Connected systems and architectures
- Security in the internet protocol stack
- Advanced access control, Public Key Infrastructures

Secure communications
- Secure IP-based communication protocols
- Secure TLS configuration
- IoT technologies: Wi-Fi, Bluetooth, BT Low Energy, NFC, ZigBee

Interface protection
- Attacks on external interfaces
- Securing interfaces

Web services
- Types and uses cases
- Access control
- Command injection

Advanced training: Automotive security

Training topics

- Get to know current aspects of automotive security
- Discover a holistic view on automotive security
- Understand the challenges and possibilities to develop secure ECUs
- Get to know the challenges and possibilities of secure networking
- Learn about the challenges and possibilities of secure connected vehicles
- Gain an overview of the most important automotive safety standards

Target group

- Product or project managers who need to establish a solid understanding about automotive security principles for secure design of ECUs, the on-board network or connected vehicle services
- Automotive product engineers who are responsible for analyzing and defining security requirements and for defining security concepts

Requirements

- Basic technical understanding of automotive systems on engineering level
- Basic technical understanding of cryptography and IT security, i.e., knowledge from secure product design or equivalent

Duration:
2 days / 16 hours

Languages:
German / English

Location:
- ETAS site
- customer site
- conference hotel
- online

Day 1

Introduction to automotive security
- Overview of automotive threats
- Review of recent successful attacks

Holistic automotive security
- Security as a process
- Security stages for a holistic security model

Secure ECU design
- Software
- Case study: AUTOSAR
- Hardware
- Case Study: SHE
- Trust anchors, key handling, and supply chain security

Day 2

Secure on-board networking
- Automotive network buses
- Network security measures
- Case study: SecOC
- Secure network architectures

Secure connected vehicles
- Automotive IoT use cases
- Protection of external interfaces

Automotive security standards
- Security activities in the automotive lifecycle
- UNECE WP.29 & ISO 21434

Technology and technical standard security trainings

Basic training: AUTOSAR security

Training topics

- General knowledge about Classic/Adaptive AUTOSAR and their security architecture
- Knowledge about security controls and their respective AUTOSAR implementation
  - Secure Communication: SecOC, TLS, IPsec
  - Crypto operations: Classic & Adaptive AUTOSAR crypto stack
  - Intrusion Detection System: AUTOSAR IdsM
  - Secure Diagnostics with service 0x27 (SecureAccess) and 0x29 (Authentication)
  - Secure Boot within Adaptive AUTOSAR: Trusted Platform
  - Access control to service interfaces with Identity & Access Management
  - Secure update of the AUTOSAR stack and applications using AUTOSAR UCM

Target group

- Security Engineers that want to use the AUTOSAR Security Building Blocks to secure their vehicle
- AUTOSAR developers that want to know more about the security features of AUTOSAR

Requirements

- Basic knowledge of security
- Background in automotive technology and knowledge of relevant security mechanisms

Duration:
1 day / 8 hours

Languages:
German / English

Location:
- ETAS site
- customer site
- conference hotel
- online

Day 1

Threats in the automotive domain
- Overview about the automotive threat landscape
- Introduction of AUTOSAR modules to address these threats

AUTOSAR overview
- Introduction of the AUTOSAR consortium
- Classic AUTOSAR and Adaptive AUTOSAR
- Deployment scenarios for Classic & Adaptive AUTOSAR

Classic AUTOSAR Security Modules
- SecOC
- TLS
- IPsec
- Crypto stack
- Intrusion Detection System
- Secure Diagnostics

Adaptive AUTOSAR security modules
- Adaptive AUTOSAR architecture
- Realization of security building blocks that are already available in Classic AUTOSAR
- Identity & Access Management
- Trusted Platform
- Secure Update

Outlook and summary
- Motivation: Change in EE architecture towards zonal architectures
- MACsec
- Firewall
- Summary

Technology and technical standard security trainings

Basic training: Information security standards and requirements catalogs

Training topics

- Introduction to Information Security Standards
- ISO 27001 (Information Security Management)
- ISO 27005 (Information Security Risk Management)
- OWASP ASVS (Application Security Verification Standard) v4.X
- OWASP MASVS (Mobile Application Security Verification Standard) v1.2
- NIST 800-53 (Catalog of Security and Privacy Controls)
- (Bosch EISA)

Target group

- Risk Managers want to learn about requirement standards and catalogs and the security goals posed by international standards
- Product Owners want to learn the basics to derive security requirements from standard catalogs

Requirements

- Basic knowledge of management systems
- Basic knowledge of security standards

Duration:
1 day / 8 hours

Languages:
German / English

Location:
- ETAS site
- customer site
- conference hotel
- online

Day 1

Motivation
- Why should you use security requirement catalogs?
- Information security vs. IT security
- CIA Triad
- Countermeasures

ISO 27001
- Management system
- Purpose of ISO27000
- What is an ISMS
- Annex A overview
  - Details of all the requirements
- Learning game, additional resources

ISO 27005
- Manage the PDCA cycle
- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment plan
- Demo time for risk handling in Jira for a project

NIST 800-53:
- NIST overview
- Walkthrough of all 20 control families
- Additional material in form of spreadsheets and structured controls

OWASP ASVS:
- Introduction
- How to use ASVS as a requirements list in your context
- ASVS levels
- Walkthrough all the categories and chapters
- Link to OWASP cheat sheet for ASVS requirements

Bosch EISA:
- Introduction
- How to use EISA as a requirements list in your context

Technology and technical standard security trainings

Basic training: Windows security

Training topics

- Learn about common attacks on Windows installations
- Explore tools like Command & Control frameworks and malware like Mimikatz that attackers might also use in the wild
- Learn to spot misconfigurations and potential for privilege escalation
- Deepen your understanding of Windows hardening options and countermeasures
- Hands-on hacking lab with exercises for all parts

Target group

- Windows administrators
- Administrators of applications or services based on Windows hosts
- Developers and architects for those systems, applications and services
- Everyone interested in evaluating the security and hardening options of Windows systems

Requirements

- Basic knowledge of Windows
- General understanding and awareness of IT-security

Duration:
1 day / 8 hours

Languages:
German / English

Location:
- ETAS site
- customer site
- conference hotel
- online

Day 1

Introduction
- Legal Disclaimer, Terms and Conditions
- Lab Environment

Network based attacks
- Reconnaissance, port scanning
- Exploitation of vulnerable services
- Brute-force attacks on Windows services
- Command and Control frameworks and malware

Local privilege escalation attacks
- Detecting misconfiguration in Windows systems and installed software
- Exploitation of misconfigured services
- Hardening options
- Anti-Virus and Anti-Virus Evasion strategies

Post exploitation
- Credential extraction with mimikatz
- Other stored credentials
- Persistence of malware
- Hardening options
- Anti-Virus and Anti-Virus Evasion / Living of the Land

Technology and technical standard security trainings

Advanced training: ISO/SAE 21434 security engineering and management

Training topics

- Learn the building blocks of ISO/SAE 21434 compliant security engineering.
- Get an overview how ISO/SAE 21434 helps you to meet the requirements of the UN regulation 155.
- Understand the risk-based approach of ISO/SAE 21434 to product security.
- Learn from our firsthand expertise for the ISO/SAE 21434 through dedicated case studies.
- Get to know more about security engineering during the concept phase (incl. cybersecurity relevance assessment, goals & concept).
- Find out about the importance of security engineering in the development phase (incl. cybersecurity DIA, design, implementation and V&V).
- Benefit from our knowledge about cybersecurity in production, operations, maintenance and decommissioning.

Target group

- Security manager, product manager or project manager
- System engineer, software engineer, hardware engineer, developer

Requirements

- Basic technical understanding of automotive systems on engineering level

Duration:
2 days / 16 hours

Languages:
German / English / Japanese

Location:
- ETAS site
- customer site
- conference hotel
- online

Day 1

Introduction to security engineering
- Motivation based on common challenges
- Context of the UNECE WP.29 regulation
- ISO/SAE 21434 overview

Governance & Ecosystem
- Cybersecurity Management System (CSMS)
- Security in the supply chain

Risk Management
- Risk assessment methodology

Day 2

Risk management (continued)
- Continuous cybersecurity activities including cybersecurity monitoring, vulnerability analysis and management

Concept and development
- Project-level cybersecurity management
- Security goals and concept
- Cybersecurity validation

Production and operation
- Production security
- Incident response and patch management
- Decommissioning

Outlook

Cybersecurity automotive professional certification

- Successful participation allows participants to receive a certification as “Cybersecurity Automotive Professional” (upon request)
- Participants prove in a 90-minute multiple-choice exam their understanding of the training contents
- The exam is conducted by the accredited certification body PersCert TÜV from the TÜV Rheinland Academy

Offboard – Enterprise security trainings and coaching

Basic training: Web application security

Training topics

- Introduction to Web Application Security covering OWASP Top10
- Knowledge about the most common vulnerabilities and their respective mitigations
  - OWASP Top10 including demos to the most common attacks
  - Vulnerabilities:
    - Injection
    - Cryptographic failures
    - Server-Side Request Forgery
    - Vulnerable and Outdated Components
    - Identification and Authentication Failures
    - Security Misconfigurations
- Hands-on Hacking Lab to learn basic penetration testing skills

Target group

- Developers that want to learn basic Web Application vulnerabilities and how to prevent them
- Architects that want to know more about the securing web applications or platforms

Requirements

- Basic knowledge of web applications
- Background in Enterprise IT technologies

Duration:
1 day / 8 hours

Languages:
German / English

Location:
- ETAS site
- customer site
- conference hotel
- online

Day 1

Motivation
- Why should Web Application Security be part of your DevOps Lifecycle
- Evolution of the World Wide Web

Introduction to Penetration Testing tools
- Overview PortSwigger Burp Suite
- Firefox / Chrome Developer Console

OWASP Top10
- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures

Security Logging and Monitoring Failures

Service-Side Request Forgery (SSRF)

More Web Application Security (short summary)

What is not covered by OWASP Top10

OWASP Application Security Verification Standard (ASVS)

OWASP Web Security Testing Guide

Web Application Hackers Handbook

Hands-on Hacking Lab

Terms and Conditions

Solve multiple hacking challenges in a web shop

Guided assistance

Advanced coaching: Security risk analysis

Coaching topics

- Learn and understand how security risk analyses contribute to efficient and effective risk management, e.g., in the context of ISO/SAE 21434
- Get to know one methodology of security risk analyses
- Carry out a security risk analysis for one of your systems

Target group

- Product and project managers who need to understand the methodology of a security risk analysis in the context of the product development process
- Security managers who are responsible for conducting security risk analyses during the product development process

Requirements

- Basic knowledge of product development processes
- General understanding and awareness of security risks
- Overview and description of the system that is to be evaluated

Workshop 1

- Why to perform a security risk analysis?
- Introduction to the security risk analysis methodology
- What are the valuable assets of your target of evaluation?

Workshop 2

- Lessons learned & results from workshop #1
- Threat analysis based on attack trees
- Assessment of attack potentials based on common criteria

Workshop 3

- Lessons learned & results from workshop #2
- What could possibly go wrong?
  - Damage scenarios
  - Damage potential assessment
- Risk handling
- Security needs
- Discussion & Q&A

In-between the workshops, the customer team completes the steps of the methodologies, while the ETAS trainer provides support and reviews.

Duration:
3 days (spread over approx. 3 month)

Languages:
German / English

Location:
- ETAS site
- customer site
- conference hotel
- online

Advanced coaching: Security testing strategy

Coaching topics

- Get to know the motivation, challenges and limitations of security testing
- Find out how to thoroughly consider security testing in the product development lifecycle (e.g., testing activities in the different phases of the lifecycle)
- Get an overview of different security testing methods and understand the differences
- Learn and understand the basic principles of security testing
- Learn and understand "what" to target in the security testing in which testing setup (e.g., systems, devices, components, interfaces)
- Get to know how to handle identified weaknesses and which mitigation options exist
- Create a first draft of a security testing strategy during the workshop
- Understand the requirements for security testing from the most prominent standards and regulations

Target group

- Product managers, project managers, test managers, and security managers who need to establish a solid understanding about security testing methods and how to apply them throughout the development lifecycle.

Requirements

- Technical understanding of systems/products and system/product development
- Basic understanding of IT security is helpful
- If available, an overview of the own security testing strategy

Duration:
1 day / 8 hours

Languages:
German / English

Location:
- ETAS site
- customer site
- conference hotel
- online

Training

- Why is practical security testing important? – Real-world example
- Security testing in UNECE WP.29 and ISO/SAE DIS 21434*
- When to test in the product development lifecycle
- Security testing methods
  - Penetration testing
  - Vulnerability scanning
  - Functional security testing
  - Code analysis
  - Fuzzing
  - Hardware / Side channel attack testing
- General security testing principles
- What to test in the automotive environment
- Handling of findings and testing resources

Workshop

- Status quo of security testing
- Which testing methods are already established? What's being used today?
- What is currently working well and where are the gaps?
- Which testing methods and tools do we want to use in the future?
- When and to what extend do we need to test?
- Who is responsible for which testing artefacts?
- What could a future security testing strategy look like?

Topics and leading questions can be tailored to customer needs.

* Content tailored for automotive customers is optional

Offboard – Enterprise security trainings and coaching

Advanced coaching: Threat modeling

Coaching topics

- Understand what a Threat & Risk Analysis / Threat Model is in general
- Get a deeper look into the four stages of performing a Threat Model with the STRIDE methodology
- Learn how to create a data flow diagram of an / your own product / service / solution including Trust Boundaries
- Learn how to identify threats with the STRIDE methodology
- Get a basic understanding how to rate identify risks or threats
- Learn how to elaborate counter or mitigation measures for each identified threat
- Understand several options how evaluate the own analysis and how to elaborate fitting action items

Target group

- Product and project managers who need to understand the methodology and output of a Threat Model
- Security managers who are responsible for performing or understand the output a Threat
- System-, software- & hardware engineer, developer.

Requirements

- General understanding and awareness of IT-security
- Knowledge about the system overview, used technologies and the communication between these components

Duration:
1 day / 8 hours

Languages:
German / English

Location:
- ETAS site
- customer site
- conference hotel
- online

Day 1

Introduction to threat modeling and the four stages
- Introduction to Step 1: Diagram
- Introduction to Step 2: Risk identification
- Introduction to Step 3: Mitigation measures
- Introduction to Step 4: Evaluation

Data flow diagrams
- Different levels of data flow diagrams
- Trust Boundaries
- Case study: Data flow diagram + Trust boundaries

Risk identification
- STRIDE
- Case study: STRIDE analysis

Day 2

Recap of day 1

Risk identification part 2
- Case study: STRIDE analysis

Risk mitigation
- Mitigation process
- Risk rating
- Case study: Risk rating
- Mitigating risks
- Case Study: Risk mitigation

Evaluation

Ready to train you worldwide

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

More information on ESCRYPT trainings:
www.etas.com/security-trainings.com

ETAS/COM2_AS/04/2023