System Security in the Automotive Industry

We can help you deliver secure, software-enabled automotive technologies that keep your passengers—and their data—safe at every turn

Modern vehicles are not only entrusted with the physical security of the passengers within them, they also act as mobile access points to sensitive personal data. Consequently, they represent a point of growing concern among drivers. As auto manufacturers increasingly rely on software to evolve the connected and autonomous vehicle landscape, they cannot afford to be complacent when it comes to application security, whether they develop applications in-house or obtain their software through a software supply chain. Weaknesses in source code, unpatched open source vulnerabilities, external interfaces, and inadequate application security practices serve as attack vectors for malicious hackers, putting your system at risk.

Make security a driving force during development and testing

Black Duck® offers proven methodologies and automated solutions to strengthen your system security posture at every stage of the software development life cycle (SDLC) and across your software supply chain. Our goal is to enable OEMs, and Tier 1 and Tier 2 providers around the world to deliver secure, software-enabled automotive technologies that keep passengers—and their data—safe at every turn. We can help you automatically detect third-party components in source code and binaries, prioritize security vulnerabilities and licenses in use, and find critical defects and weaknesses in code during development. We also support the design phases of your development life cycle by identifying the design flaws, control defects, and asset vulnerabilities that define the overall risk to your system.

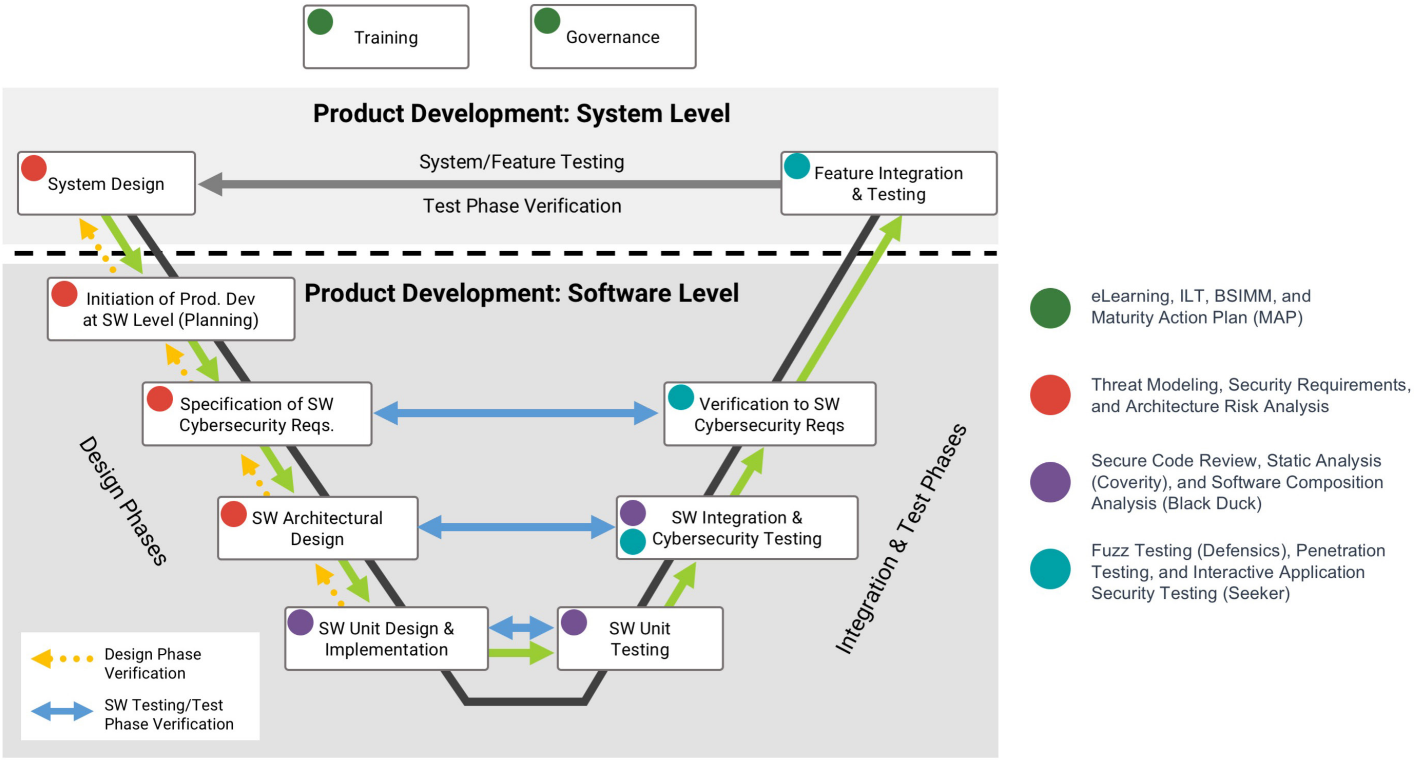
Manage risk across the development life cycle and supply chain

Our approach to automotive system security is grounded in the fundamentals of technology risk management. Black Duck supports the distinct needs of the automotive industry by performing critical activities for automotive organizations, including

- Bus analysis, fuzz testing, and reverse engineering
- Vehicle ecosystem threat modeling and architectural risk analysis
- Embedded code reviews, penetration testing, and reverse engineering
- Communications interface testing (onboard, wireless, dealer, manufacturing)
- Telematics, infotainment, and head-unit testing
- Certificate, encryption, key store analysis, and testing
- Program design and development
- Software security training

Address safety and security across development life cycles

We understand your system development life cycle and the impact security has on safety and quality.


Training
Governance
Product Development: System Level
System Design
System/Feature Testing
Test Phase Verification
Feature Integration & Testing
Product Development: Software Level
Initiation of Prod. Dev at SW Level (Planning)
Specification of SW Cybersecurity Reqs.
Verification to SW Cybersecurity Reqs
SW Architectural Design
SW Integration & Cybersecurity Testing
SW Unit Design & Implementation
SW Unit Testing
Design Phases
Integration & Test Phases
Design Phase Verification
SW Testing/Test Phase Verification
eLearning, ILT, BSIMM, and Maturity Action Plan (MAP)
Threat Modeling, Security Requirements, and Architecture Risk Analysis
Secure Code Review, Static Analysis (Coverity), and Software Composition Analysis (Black Duck)
Fuzz Testing (Defensics), Penetration Testing, and Interactive Application Security Testing (Seeker)

Achieve excellence in automotive system security

Tools	Find vulnerabilities in your software stack with our industry-leading tools. • Static analysis (certified for ISO 26262, supports MISRA and AUTOSAR coding guidelines) • Fuzz testing to ensure ISO 21434 compliance (supports CAN, CAN-FD, DoIP, SOME/IP, etc.) • Interactive application security testing • Software composition analysis to detect third-party and open source components in source code and binaries, track and remediate vulnerabilities during development and in containers in production, identify third-party licenses, and set policies to avoid noncompliance
Embedded penetration testing	Verify the functional and security performance of embedded systems (e.g., ECUs) and identify vulnerabilities in the embedded software stack.
Architecture and design	Find architectural, design, and system defects and flaws with architecture risk analysis and threat modeling.
Training	Educate your developers to become more security aware with our security training courses delivered as instructor-led, eLearning, and virtual classes.
Assessment	Assess your level of program maturity with Building Security in Maturity Model (BSIMM), a Maturity Action Plan, security metrics, and our software security initiative programs.

Auto industry participation

We are committed to the evolution and adoption of cybersecurity best practices in the automotive industry, and we practice our commitment by contributing to a range of industry groups.

Define a strategy to address system risks

Increase visibility

- Identify weaknesses and shortcomings in development and testing practices
- Distribute security insight throughout the SDLC and into production

Shift left

- Incorporate quality, security, and safety throughout the SDLC
- Detect early without slowing development

Automate

- Avoid delays and potential human failure with continuous testing
- Establish triggers, workflows, and policies

Manage and maintain

- Manage and monitor vulnerabilities and defects
- Track the transfer of risk throughout the software supply chain

Remove friction

- Build in security and quality
- Integrate into development workflows

Establish awareness

- Maximize security awareness among employees
- Augment security skill sets and share investment in the outcome

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.