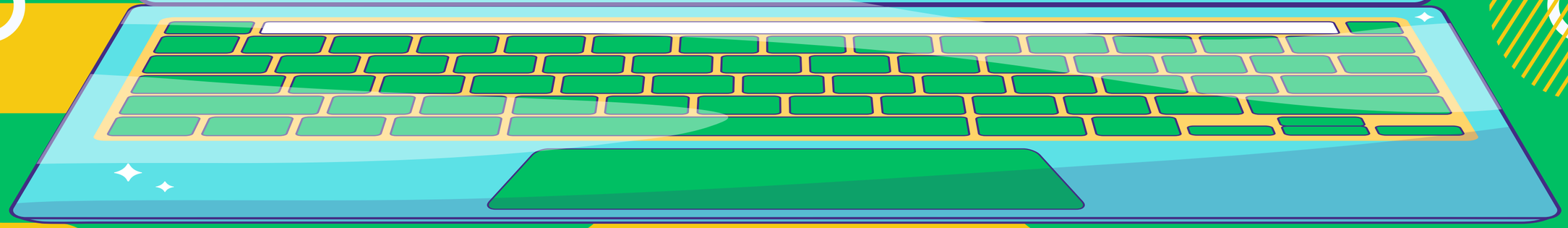
INTEGRATING
SECURITY BEST PRACTICES
WITH **SHIFT-LEFT** AND **SHIFT-RIGHT**
IN **AGILE SDLC**



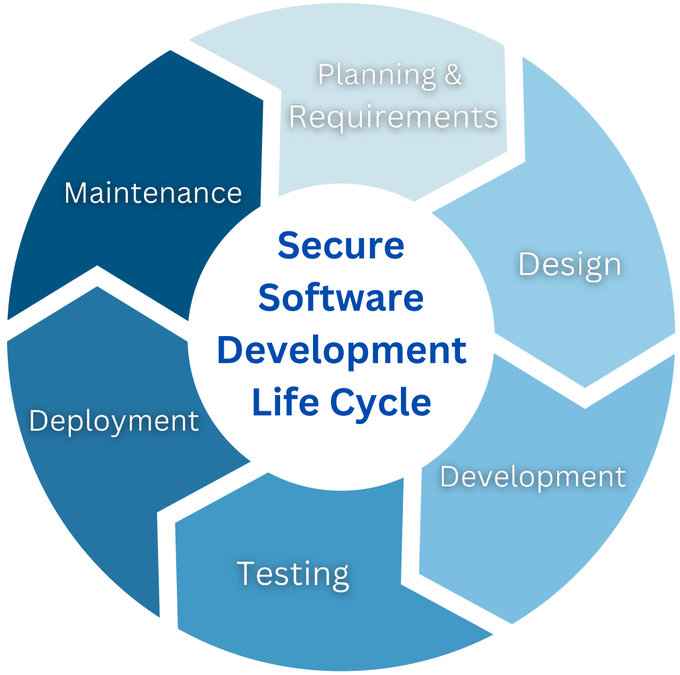
Presented by Liliya Frye

AGENDA

- Agile SDLC
- Security Testing
- Shift-Left & Shift-Right
- SAST/SCA
- DAST
- IAST
- Challenges
- Solutions

AGILE SDLC

Good Fast Cheap Done

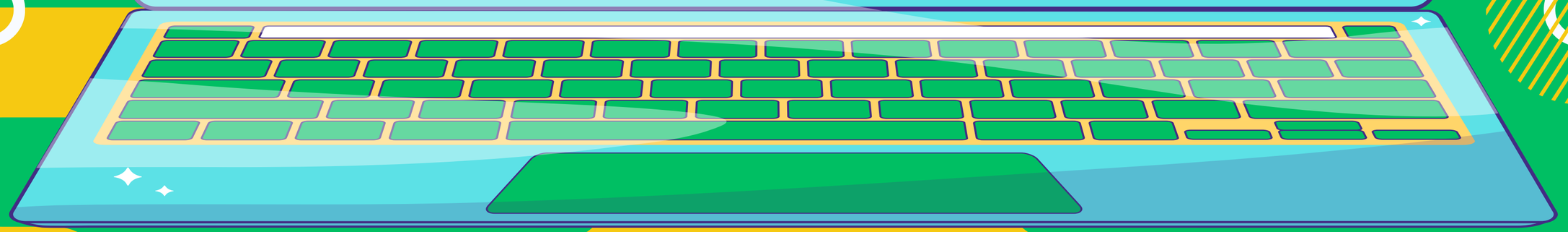


LiliyaFrye.com

SECURITY TESTING

Types of Security Testing:

- **Static Application Security Testing (SAST)**: Analyzes source code or bytecode for vulnerabilities without executing the code
- **Dynamic Application Security Testing (DAST)**: Tests the application in its running state, simulating external attacks
- **Interactive Application Security Testing (IAST)**: Monitoring of deployed applications in real-time and reporting security weaknesses found in custom code and 3d party libraries
- **Software Composition Analysis (SCA):** Analyzes open-source components and libraries for risk and license compliance issues
- **Penetration Testing:** Simulates real-world attacks to identify exploitable vulnerabilities
- **Security Auditing:** Reviews and analyzes systems and processes to ensure they meet security standards, regulations and compliances



LiliyaFrye.com

SHIFT-LEFT AND SHIFT-RIGHT

"Bugs are cheap when caught young" - Larry Smith, the founder of Shift-Left

Shift-Left

- Unit and Integration Testing (CI/CD)
- Static Application Security Testing (CI/CD)
- Software Composition Analysis (CI/CD)
- Interactive Application Security Testing (CI/CD)

Shift-Right

- Testing and monitoring in Production
- Canary releases to a small group of users
- Dynamic Application Security Testing (+ pre-prod)
- Chaos Engineering (Fuzz Testing)
- Penetration Testing (+ pre-prod)

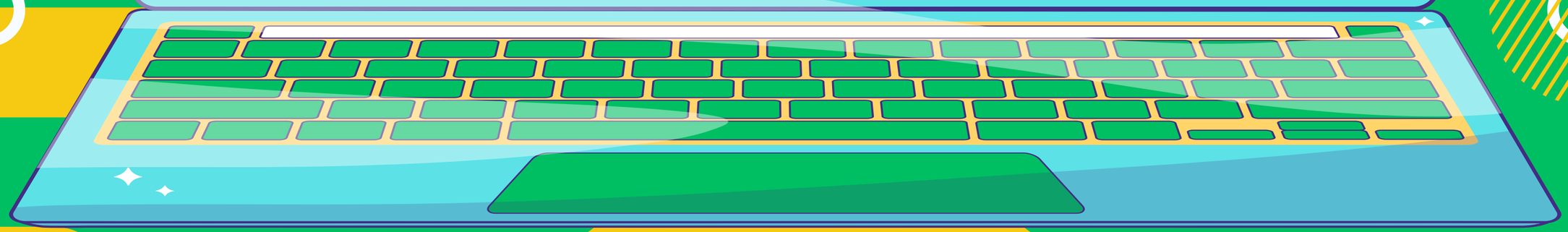
LiliyaFrye.com

SAST / SCA

SAST: White box tesing - analyzes source code, byte code and binaries for issues without executing the code

SCA: White box tesing - analyzes open-source components and libraries for risk and license compliance issues

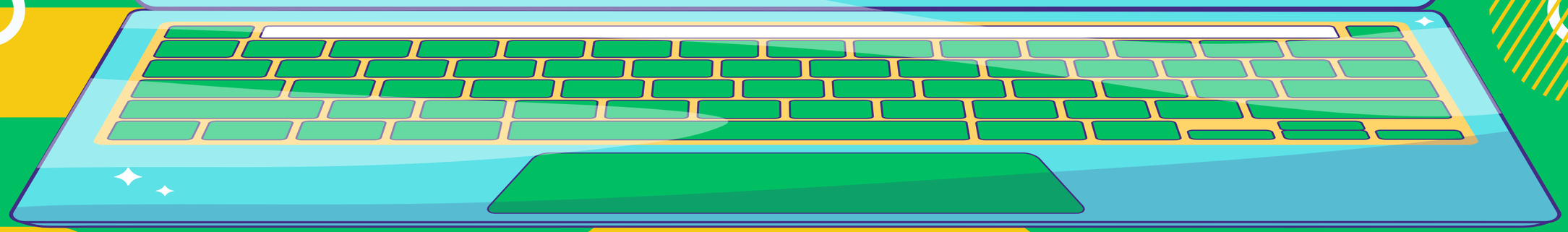
Tool	Key Features
Sonar: SonarCloud SonarQube	• Scans dependencies and libraries at a level that other tools miss • Supports over 30 languages and many frameworks • Automated code scanning with real time feedback • Comprehensive reporting utilizing the OWASP Top 10 and PCI DSS standards to ensure consistency • Utilization of AI/ML to optimize analysis processes, ensuring that they are as efficient and precise • Integrates with GitHub, GitLab, Bitbucket Cloud, Azure DevOps
Checkmarx	• Offers Codebashing AppSec Training for OWASP members • Supports over 35 languages and 100+ frameworks • Smooth integration with IDEs and CI/CD • AI guides engineers by identifying vulnerabilities and assisting with remediation in the code • Scans ensure that OWASP Top 10, PCI DSS, ASD STIG, OWASP Top API, NIST standards are enforced • Vulnerability prioritization allows developers to understand the risks & severity of each issue flagged



DAST

Dynamic Application Security Testing (DAST): Black box testing - tests the application in its running state, simulating external attacks

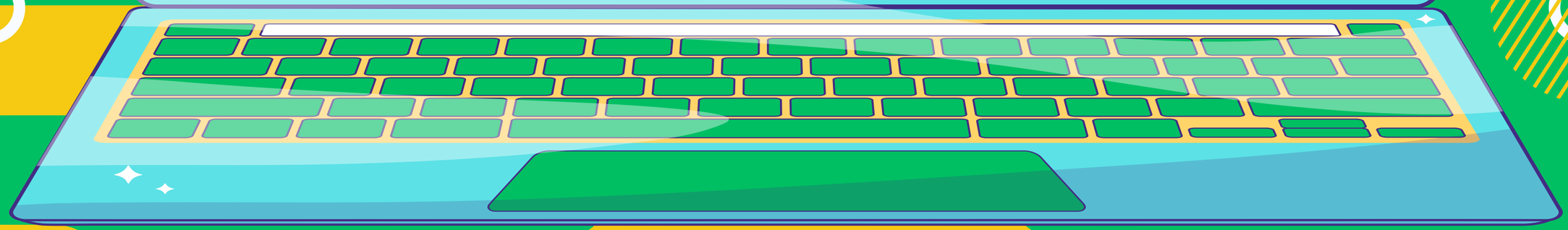
Tool	Key Features
ZAP	• Identifies vulnerabilities in web apps through both active and passive scanning techniques • Automatically detects issues such as SQL injection, XSS, and other OWASP Top 10 without access to the code • Generates detailed reports with prioritized issues, including risk ratings and remediation advice • Includes specialized capabilities for testing the security of APIs (RESTful APIs), SPAs, WebSockets • Integrates with CI/CD, enabling automated security testing throughout SDLC • Offers browser-based crawling & scanning for dynamic content with custom tests using JavaScript • Combines DAST with IAST capabilities to enhance vulnerability detection with real-time feedback
Checkmarx	• AI guides engineers by identifying vulnerabilities and assisting with remediation • Smooth integration with IDEs and CI/CD, enabling automated security testing through SDLC • Scans ensure that OWASP Top 10, PCI DSS, ASD STIG, OWASP Top API, NIST standards are enforced • Vulnerability prioritization allows developers to understand the risks & severity of each issue flagged • Provides remediation guidance and the optimum place for the code to be fixed • Incorporates business context to assess the real-world risk of issues to prioritize remediation based on potential impact



IAST

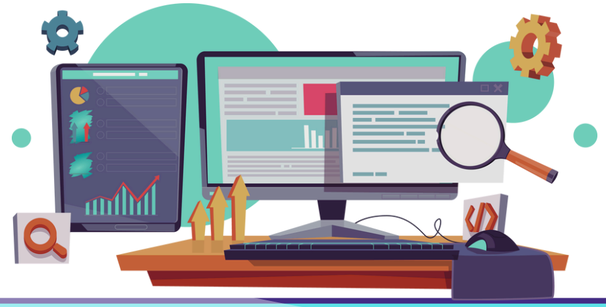
Interactive Application Security Testing (IAST): Grey box testing - hybrid of SAST & DAST with sensors that can directly monitor & observe apps behavior during execution

Tool	Key Features
Contrast Security	• Supports apps written in 35 programming languages and many frameworks • Instantly identifies vulnerabilities and provides solutions during runtime • Provides precise vulnerability identification, minimizing false positives through real-time analysis • Easily integrates with existing CI/CD pipelines and development tools for Continuous Security • Identifies AI Security threats, including OWASP Top 10 for Large Language Models Applications • Runtime Application Self-Protection capabilities for automatic protection against real-time threats
Veracode	• Supports apps written in Java and .Net • Provides actionable insights and remediation guidance directly to developers within their workflows • Designed to scale across large organizations, offering consistent security across all applications • Allows organizations to enforce security policies and track compliance across the SDLC • Offers in-depth reporting and analytics to track security posture and identify high-risk areas • Simulates attacks in real-time from OWASP Top 10 threats



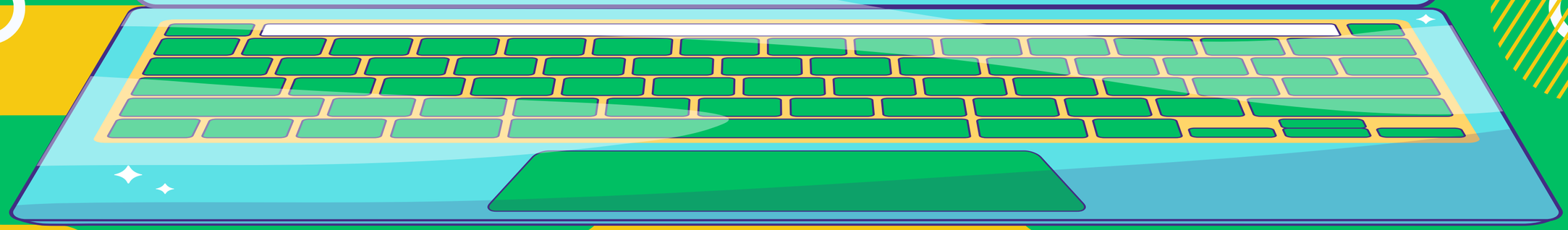
CHALLENGES

- Complexity in Implementing Shift-Left & Shift-Right
- Tool Integration and Compatibility
- Automation Challenges in Security Testing
- Ensuring Comprehensive Coverage
- Maintaining Compliance and Regulatory Standards
- Skill Gaps and Training Needs



SOLUTIONS

- **Quality** and **Security-First** culture
- **Encrypt data** at rest and in transit
- Improve **code quality** with **secure coding** practices
- Use **lightweight AI-powered tools** that support **Shift-Left**
- Configure the **CI/CD to auto trigger security tests** upon **code commits, pull requests** and **deployment** events
- Integrate security tools with **issue tracking systems** (Jira, Gituhb Issues, etc.) and **generate reports**
- Combine automated testing with manual exploratory **penetration testing**
- **Bring in experts** for workshops to **enhance** the team's **security knowledge**
- **Continuously monitor** and **continiously improve**

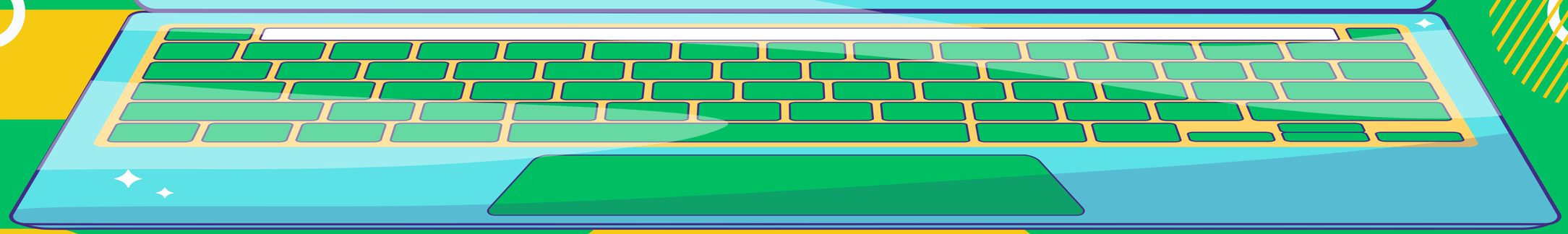


LiliyaFrye.com

THANK YOU

- Thank you OWASP LA for organizing the event
- Thank you Checkmarx for sponsoring the event
- Thank you HiveWatch for hosting the event

- Connect with Liliya on LinkedIn
- Subscribe to Women In Tech Newsletter and read the inspiring stories of women in tech
- Book a workshop (for organizations)
- Book 1on1 tech consultation with Liliya
- Commission Liliya to write technical articles about your product with clarity and expertise
- Join the movement with Women In Tech Merch



LiliyaFrye.com