



Live Events Catalog

Sessions, series, and speakers for builders and Security Champions

Security Champions grow fastest when they learn from the people who write the standards they use. Katilyst live events bring practitioners from OWASP projects, EU standards work and industry security teams into the virtual room with your builders. Every session is tailored to your environment, policies and culture. Browse by audience, choose a ready-made series, or ask us to design something new.

Part 1: For Builders

Sessions for the developers, architects and Security Champions who design, write and ship your software. Each one is grounded in current standards and ends with practices teams can use in their next sprint. Each session lasts 60-90 minutes, including time for audience Q&A.

Track 1: AI-Assisted and Agentic Development

Build with AI assistants and agents while keeping control of what they write and what they can do.

GenAI & LLM Fundamentals for Builders

Teams are shipping features on large language models before anyone has mapped the new attack surface. This session explains how LLM applications work and walks through the [OWASP Top 10 for LLM Applications \(2025\)](#), from prompt injection and sensitive data disclosure to excessive agency.

Secure AI-Assisted Development

AI coding assistants now write a large share of new code, and they repeat insecure patterns as fast as they generate. This session covers reviewing AI-generated code, the anti-patterns assistants produce most often, and the prompts, policies and pipeline checks that keep human judgment in the loop.

Securing AI Agents

Agents plan, call tools and act with real credentials, so one injected instruction can become a real action in production. Using the [OWASP Top 10 for Agentic Applications \(2026\)](#), this session covers goal hijacking, tool misuse, identity and privilege abuse, memory poisoning, and the architecture patterns that contain them.

MCP and Tool Integration Security

The Model Context Protocol makes it easy to connect agents to internal systems, and every connection is a trust decision someone should make on purpose. This session covers authenticating and scoping MCP servers, vetting third-party tools, and logging agent actions so they can be investigated.

GenAI Data Protection for Builders

Prompts, training data, embeddings and model outputs all carry sensitive data, and each one leaks in its own way. This session covers classifying data in AI pipelines, access control on vector stores, output filtering, and producing the evidence data protection reviews ask for.



Track 2: Web and API Vulnerabilities

The flaws attackers find most often in web applications and APIs, and the code-level defenses that stop them.

OWASP Top 10:2025

The OWASP Top 10 is the shared language between developers, testers and auditors, and the [2025 edition](#) brings Software Supply Chain Failures and Mishandling of Exceptional Conditions onto the list. This session walks each category with real examples and the controls that prevent it.

OWASP Top 10 Proactive Controls

Proactive Controls is OWASP's list of the defenses every developer should build in from the first commit, from access control to secure defaults. This session turns each control into concrete patterns for the team's own frameworks and code review checklists.

XSS: Why It Still Matters

Cross-site scripting remains one of the most common web vulnerability findings, and modern frameworks only prevent it when teams use them as intended. This session covers reflected, stored and DOM-based XSS, the framework escape hatches that reintroduce it, output encoding, and Content Security Policy.

CSRF and Clickjacking

Browsers send a user's session along with requests the user never meant to make. This session shows how CSRF and clickjacking exploit that behavior, then covers the token, SameSite and framing defenses developers can apply in their own code.

Server-Side Request Forgery (SSRF)

SSRF turns an application's own servers into a path into internal networks and cloud metadata services. This session covers finding SSRF in code and testing, allow-listing outbound requests, and the network controls that limit damage in cloud environments.

Injection Prevention: SQL, Command and Template

Injection still ranks in the OWASP Top 10:2025 because string-built queries and commands keep reaching production. This session covers parameterized queries, ORM pitfalls, command and template injection, and least-privilege database access.

Trust Boundaries and Untrusted Input

Most serious vulnerabilities begin where data crosses a boundary without being checked. This session covers finding trust boundaries in an architecture, input validation, safe deserialization, and abuse of business logic.

Secure File Uploads

Upload features accept arbitrary content from strangers and store it somewhere the application trusts. This session covers file type validation, isolated storage, malware scanning, and serving user files safely.

API Security and the OWASP API Top 10

APIs carry most application traffic today, and broken object-level authorization is the most common way they fail. Using the OWASP API Security Top 10 (2023), this session covers object- and function-level authorization, authentication, rate limiting, and secure REST design.



ReactJS Security

React blocks many injection bugs by default, and a handful of well-known escape hatches switch that protection off. This session covers raw HTML rendering, URL handling, token storage, component security and server-side rendering risks.

Track 3: Identity, Sessions, Secrets and Cryptography

Get identity, sessions, secrets and encryption right, where small mistakes hand attackers the keys.

Authentication and Authorization

Broken access control sits at number one in the OWASP Top 10:2025, and authentication failures appear at number seven. This session covers password storage, MFA, RBAC and ABAC models, SSO, and enforcing authorization consistently on the server.

Session Management

A stolen session token works like a password and skips MFA entirely. This session covers token generation, storage, expiry and rotation, and preventing session fixation and hijacking.

OAuth and OIDC Without the Confusion

OAuth delegates access and OpenID Connect proves identity, and treating one as the other produces serious login flaws. This session covers the main flows, PKCE, token validation, and the expanded OAuth and OIDC requirements in ASVS 5.0.

Digital Identity Foundations

Every access decision depends on proving who, or what, is on the other end. This session covers identity proofing, authenticators, federation and machine identities, aligned with NIST SP 800-63.

Secrets Management

Every credential committed to a repository is one clone away from being public, and rotating it takes someone's weekend. This session covers vaults, managed identities, secret scanning in pipelines, and shipping builds whose defaults are safe.

Applied Cryptography and TLS

Cryptographic failures rank fourth in the OWASP Top 10:2025, and most come from misusing sound algorithms. This session covers choosing algorithms and libraries, key management, TLS configuration, certificate lifecycle and forward secrecy.

Track 4: Secure Design and Architecture

Design choices that remove whole classes of vulnerabilities before the first line of code.

Threat Modeling 101

Threat modeling finds design flaws while they are still cheap to fix. Using STRIDE and four simple questions (what are we building, what can go wrong, what will we do about it, did we do a good job), attendees map data flows, identify likely attackers and valuable assets, and choose mitigations.



Secure-by-Design and Secure-by-Default (ENISA)

Secure-by-default means the safe configuration is the one that ships. This session translates ENISA principles into decisions made in product design and code review, and shows how regulations such as the EU Cyber Resilience Act now write them into law.

Secure Coding Practices

Most vulnerabilities come from a small set of repeatable coding habits. This session covers input validation, output encoding, error handling, and choosing vetted libraries and framework defaults, with examples in the team's own language.

Secure Error Handling and Logging

Mishandling of Exceptional Conditions is new in the OWASP Top 10:2025, and the logs that help investigate an incident can also leak tokens and customer data. This session covers failing closed, logging enough to investigate, and keeping secrets and PII out of output.

Concurrency Safety

Race conditions rarely surface in code review or tests, so they reach production and stay there. This session covers shared mutable state, atomicity, idempotency and cache coherence, and what a passing load test does and does not prove.

Unmanaged and Low-Level Vulnerabilities

Memory safety issues now live in the native libraries, drivers and firmware beneath managed code. This session covers what goes wrong below the runtime and how to reason about risk in code the language was supposed to protect.

Privacy Engineering

Privacy requirements become design decisions long before they reach legal review. This session covers privacy principles such as data minimization and purpose limitation, privacy-aware data flow diagrams, and privacy threat modeling with LINDDUN.

Cloud Security for Application Teams

Security Misconfiguration ranks second in the OWASP Top 10:2025, and in the cloud application teams now own most of that configuration. This session covers least-privilege IAM, storage exposure, network boundaries and managed service defaults.

Secure Configuration Management

Servers and services drift from their hardened baseline one quick fix at a time. This session covers hardening baselines, patch management, configuration as code and drift detection.

Infrastructure as Code, Containers and Kubernetes

Infrastructure definitions and container images now ship through the same pipelines as application code, with the same chance of carrying flaws. This session covers IaC scanning, image hygiene, Kubernetes RBAC and admission policies.



Track 5: Testing, Tooling, and Supply Chain

Tools, tests and supply chain practices that catch problems early and keep them fixed.

SAST and DAST That Developers Trust

SAST and DAST each find different issues, and either one will bury a team in findings if it is switched on without a plan. This session covers what each tool can see, tuning rules, and building a pipeline developers keep paying attention to. We can also include SCA, RASP, and IAST into this session, if desired.

Security Unit Tests, Abuse Cases and Regression Tests

A test suite usually proves a feature works when used correctly. This session covers writing abuse cases alongside user stories, turning them into automated tests, and keeping fixed vulnerabilities fixed.

Software Supply Chain Security

Software Supply Chain Failures ranks third in the OWASP Top 10:2025, driven by attacks on public registries such as npm and PyPI. This session covers SBOMs, vetting third-party packages, detecting typosquatting and poisoned updates, and verifying provenance.

CI/CD Pipeline Security

Build pipelines hold production credentials and run third-party code on every commit. This session covers the OWASP Top 10 CI/CD Security Risks, hardening runners and third-party actions, and signed, verifiable builds using SLSA.

DevSecOps: Security in the SDLC

Security activities work best when each one has a natural home in the delivery process. This session maps practical checks to each stage from requirements to release and shows how to add them while keeping delivery speed.

Better Bug Reports

A clear security bug report saves hours of back-and-forth between reporters, developers and operations. This session covers a reporting standard with examples, aligning reporters with delivery teams, and prioritizing the resulting work.

Mobile App Security

Mobile apps run on devices the business does not control and store data where attackers can reach it. This session covers the OWASP MASVS, secure local storage, certificate pinning, and platform permissions.

Track 6: Security Champion Skills

Practical skills for Security Champions: leading threat models, influencing peers, and making the role last.

The Security Champion Role: Getting Started

New Security Champions often receive the title before a clear picture of the job. This session covers what the role involves week to week, how much time it takes, where to get help, and early wins that build credibility with the team. We build the details of this session with you, ensuring the content is aligned to your program goals.



Influencing Without Authority

Security Champions rarely own the roadmap, so their impact depends on persuasion. This session covers framing risk in product and delivery terms, choosing which issues to push, and handling pushback constructively.

Facilitating a Threat Model on Your Team

Threat modeling scales when Security Champions can run sessions without an AppSec engineer in the room. This session covers scoping, running a 60-minute session, keeping everyone engaged, and turning findings into tickets that can be prioritized in your product backlog.

Security for Product Managers

Product managers decide what gets built and when, which makes them the earliest security decision-makers in the process. This session covers writing security requirements and abuse cases into user stories and weighing risk during prioritization.

Part 2: For Security and Program Leaders

Sessions for the leaders who build, fund and answer for security programs. They cover how to measure and mature a program, and what new regulation requires of the software you ship. Each session lasts 60-90 minutes, including time for audience Q&A.

Track 7: Program Maturity and Standards

Frameworks, metrics and behavior science for an AppSec program that improves year over year.

Building a Lasting AppSec Program with OWASP SAMM

Many SAMM efforts stall between the first assessment and the second, when the roadmap exists and nobody owns the work. This session covers preparing the organization, running assessments that keep goodwill, scoping roadmaps so they stay owned, and the change management that decides whether progress lasts.

OWASP SAMM and BSIMM Compared

BSIMM describes what a set of firms actually do, and SAMM describes what a program should be able to do. This session compares the two on structure, evidence model and cost, and shows what each can justify to an auditor or a board.

OWASP ASVS 5.0 in Practice

ASVS 5.0, released in May 2025, defines what "secure enough" means requirement by requirement across roughly 350 requirements and three levels. This session covers the new structure, choosing a verification level honestly, and using the machine-readable release in contracts, testing and procurement.

Auditable Application Security Controls with ISO/IEC 27034

To an auditor, a control without evidence looks the same as a missing control. This session uses the ISO/IEC 27034 organization normative framework to design application security controls that produce their own evidence.



Designing an SCA Program That Keeps Up

Most SCA programs struggle with throughput: the scanner works, the queue grows, and triage capacity sets the exposure window. This session covers designing for flow, using reachability and exploitability to cut what reaches a person, placing ownership where upgrades happen, and measuring time to fix.

AppSec Habits That Stick: Applying Behavior Science

Many controls hold only while someone enforces them; switch off the blocking gate and see what remains. This session applies behavior science to secure development, covering why training alone rarely changes behavior, what shifts defaults, and how to build practices that outlast their champion.

Application Risk Rating

Consistent risk ratings decide which applications get attention first. This session covers rating models, inputs such as data sensitivity and exposure, and the extra factors to weigh for applications built with or powered by GenAI.

AI in Security Audit and Assurance

GenAI can speed up evidence gathering, analysis and report drafting, and it can also introduce errors an auditor must catch. This session covers practical uses, accuracy checks, and the controls that keep AI-assisted findings defensible.

Governance and Risk Management

Security investment needs a governance frame that leadership recognizes. This session covers NIST CSF 2.0 and ISO/IEC 27001 structures, regular risk assessment and testing, and balancing security spend with business goals.

Measuring Security Culture and Champion Programs

Programs lose funding when they cannot show results in terms leadership trusts. Drawing on data from the Katilyst State of Security Champions Report, this session covers leading and lagging indicators, participation and behavior metrics, and reporting that keeps budget.

Leading Engineering Teams Through the Agentic SDLC

AI agents are changing how software gets planned, written and reviewed, and every role on an engineering team is shifting with them. This session covers the emerging agentic SDLC, where human judgment stays essential, and the change management that brings teams along.

Track 8: Regulation and Compliance

What the CRA, the EU AI Act and industry frameworks require - and the engineering work behind them.

EU Cyber Resilience Act: Overview and Requirements

The CRA makes product security a condition of selling into the EU, and its reporting duties have applied since 11 September 2026: a 24-hour early warning and a 72-hour notification for actively exploited vulnerabilities and severe incidents. This session covers scope, product classes, secure-by-design requirements, vulnerability handling and the main obligations arriving 11 December 2027.



The CRA and Your Open Source Dependencies

CRA obligations land as documentation, default configurations, update mechanisms and a reporting deadline the on-call team must meet. This session follows the regulation from a builder's point of view, from product classification through harmonized standards, and ends on managing open source components under the Act.

CRA Vulnerability Handling and Reporting Readiness

A manufacturer cannot report within 24 hours what it cannot detect and triage within 24 hours. This session covers building a product security incident response process, coordinated vulnerability disclosure, SBOM-driven exposure checks, and rehearsing the CRA reporting clock.

The EU AI Act for Builders

The AI Act reaches any system whose output is used in the EU, and its timeline changed when the Digital Omnibus on AI entered into force on 27 July 2026. This session covers which systems are in scope, the transparency and prohibited-practice duties already in effect, and the high-risk obligations due 2 December 2027 (standalone) and 2 August 2028 (embedded in regulated products).

SOC 2: Preparing for and Running an Audit

A SOC 2 audit touches engineering, IT, HR and legal, and surprises usually come from evidence nobody owned. This session covers Type 1 and Type 2, which teams are involved, evidence collection, and running the audit to a clean report.

Third-Party Risk Assessments

Every vendor with access to data extends the attack surface. This session covers third-party risk concepts and process, common vendor risks and the controls that address them, working with vendors on evidence, and frequent pitfalls.

Part 3: For Everyone

Security sessions for the whole organization, with no technical background required. Each is tailored to your policies, your tools and the threats your people face. Each session lasts 60-90 minutes, including time for audience Q&A.

Track 9: Security Awareness

Everyday habits that protect people and data, from spotting AI-powered scams to reporting incidents quickly.

AI Threats Everyone Should Recognize

Generative AI has made scams, fake documents and deepfake audio and video cheap to produce and hard to spot. This session explains the basics of how these tools work, shows current examples of AI-enabled fraud, and teaches simple verification habits.

Using AI Tools Safely at Work

Employees paste code, contracts and customer data into AI tools every day, often without knowing where it goes. This session covers approved versus unapproved tools, what data never goes into a prompt, checking AI output before using it, and the company's own AI policy.



AI-Powered Social Engineering

Attackers now clone voices, fake video calls and impersonate staff to IT help desks to reset passwords and MFA. This session walks through recent attack patterns, the warning signs, and call-back and verification routines that stop them.

Data Privacy Fundamentals

Every employee handles personal data, and most privacy incidents start with an ordinary mistake. This session covers data classification, least privilege, sharing and retention rules, and what to do after sending something to the wrong person.

Passwords, Passkeys and MFA

Stolen and reused credentials remain a leading cause of breaches. This session covers password managers, passkeys, MFA fatigue attacks, and how to protect personal and work accounts.

Device Security

Laptops and phones carry company data into homes, cafes and airports. This session covers updates, encryption, screen locks, public Wi-Fi, and the client's own BYOD and corporate device policies.

Safe Social Media Use

Attackers study public profiles to craft targeted scams and map an organization's people. This session covers what not to post, recognizing social media scams and fake profiles, and how misinformation, including state-backed campaigns, spreads.

Role-Based Security Awareness

Finance, sales, support and HR each face different attacks and handle different data. This session tailors threats, examples and safe practices to the departments in the room.

Incident Response Fundamentals

Fast, correct reporting shapes how much damage an incident does. This session covers what counts as an incident, severity criteria based on the client's own definitions, the role of asset inventory, and each person's part in the response.



Part 4: Interactive Events

Facilitated events of two to six hours where teams practice security together through games, competitions and hands-on labs. Katilyst supplies the facilitator, the scenarios and all tooling.

Track 10: Games and Competitions

Collaborative games and friendly competitions that build skills and energy across teams.

Threat Model Your Home (2-3 hours)

A gentle first step into threat modeling. Using STRIDE, participants threat model a house together, then apply the same method to an open source application or one of the client's own services.

Roll for Initiative: A D&D Threat Modeling Campaign (3-4 hours)

Participants follow a Dungeons and Dragons campaign structure: they map their world (system diagram), face monsters (threats), choose weapons (mitigations), and earn XP along the way. It suits teams who have done the basics and want practice that sticks.

The Great Phish-Off (2-3 hours)

Teams compete to write the most convincing phishing email, using tips and templates provided, and a judges' panel chosen with the client scores the entries. Typically built for Cybersecurity Awareness Month in October.

Social Engineering Live (2 hours)

A facilitated session where participants spot and respond to live social engineering attempts across email, chat, phone and AI chatbots.

Incident Response Tabletop (2-3 hours)

A realistic scenario unfolds in stages while leaders and responders decide what to do next, with a facilitator injecting complications. The debrief turns gaps into owned actions and can double as CRA reporting rehearsal.

Track 11: Hands-on Labs

Realistic, safe environments where developers attack and defend applications with live scoring.

Capture the Flag with OWASP ZAP (3-6 hours)

Participants attack a purpose-built vulnerable website with full authorization, exploring its features to find paths to admin rights and user data. They leave knowing how attackers think and how to use ZAP in their own testing.

Cyber Ranges with CMD+CTRL (variable duration)

Through Katilyst's partnership with CMD+CTRL, developers practice in realistic vulnerable applications with real-time scoring. Program owners receive a results map with metrics and learning plans. Seat-based pricing, facilitator optional.

GenAI and Deepfakes Workshop (2-3 hours)

Participants use text and image generation tools, then create and try to detect deepfakes. The discussion covers what this means for verification, audit and fraud controls.



Suggested Series

Not sure where to start? Check out our outcome-focused curriculum tracks.

Series	Sessions (in order)	Outcome	Best for
Security Champion Onboarding	The Security Champion Role: Getting Started → OWASP Top 10:2025 → Threat Modeling 101 → Secure AI-Assisted Development → Capture the Flag with OWASP ZAP	New Security Champions share a common baseline and have practiced it hands-on	Program launches and new cohorts
Building with AI Safely	GenAI and LLM Fundamentals for Builders → Secure AI-Assisted Development → Securing AI Agents → GenAI & Deepfakes Workshop	Teams adopting coding assistants and agents know the risks and the guardrails	Engineering orgs rolling out AI tools
EU Readiness	EU Cyber Resilience Act: Overview → CRA Vulnerability Handling and Reporting Readiness → The EU AI Act for Builders → Secure-by-Design and Secure-by-Default → OWASP ASVS 5.0 in Practice	Product and engineering leaders understand obligations, dates and the engineering work behind them	Companies selling software into the EU
Cybersecurity Awareness Month	AI Threats Everyone Should Recognize → AI-Powered Social Engineering → Passwords, Passkeys and MFA → The Great Phish-Off	A month of all-staff activity with a competitive finale	October campaigns

Speakers

Katilyst partners with a variety of thought leaders in the application security and security awareness industries, facilitating thoughtfully curated talks on a variety of important topics. Here are some of the great professionals we work with today:

Connie Matthews Reynolds

Connie is the Founder and CEO of ReynCon, a cybersecurity training and consulting provider. She is a passionate cybersecurity and technology expert who has worked in the industry for over 25 years. Under Connie's leadership, ReynCon is dedicated to transforming businesses through comprehensive InfoSec/Cybersecurity training and development. Connie's contributions to the Ohio tech industry have not gone unnoticed. She has been honored as one of the 11 recipients of Verizon's inaugural Ohio Trailblazers Award, a testament to her innovative approach and leadership. Her excellence in cybersecurity has also earned her recognition as a finalist for the prestigious Cyber Security Woman of The World and Cyber Security Woman Volunteer awards.



Jason Montgomery

Jason is an Application Security practitioner and entrepreneur with 15+ years of software engineering and security experience. He co-founded Nexosis, an automated machine learning platform acquired by DataRobot in 2018, where he served as VP of Enterprise Security for three years. He served as CTO of Mantium, an AI Safety and Security platform, and following his role there has moved into consulting in the GenAI space for the past two years, helping organizations develop and secure agentic architectures, navigate secure AI implementation and development practices. His combined expertise in programming, security, and AI provides a practical perspective on secure AI-assisted development. Jason holds two patents and has contributed to technical publications through Wiley Publishing.

Tim Chase

With over 20 years of experience in the cybersecurity industry, Tim has built and led Cybersecurity teams to support the security industry and provide value to the business. His mission is to bridge the gap between Marketing, Product, and Sales, and to help teams understand the value a Cybersecurity team and product can provide. As a former Field CISO for Lacework, Veza, and Orca Security, Tim has been at the forefront of building resilient security culture in organizations of all shapes and sizes. He is the Founder and vCISO for Continuous Security, helping small to medium-sized businesses build security programs that are practical and scalable.

Jim Manico

Jim Manico is the founder of Manicode Security, specializing in training developers in secure coding, security engineering, and AI security practices. He is an active investor/advisor with Semgrep, EdgeScan, Nucleus Security, Defect Dojo, RAD Security and others. A recognized speaker and author of "Iron-Clad Java: Building Secure Web Applications", Jim continues to lead industry standards through OWASP initiatives.

Darren Meyer

With 20 years in Application Security and related fields, Darren has focused his career on translating complex security concepts into actionable insights for a variety of audiences. He's built security programs across cybersecurity, retail, and banking verticals, complemented by nearly a decade in security research. His specialty is building bridges between technical complexity and practical application. He currently works as a security researcher with Checkmarx, prior to which he led security research and software assurance at Endor Labs.

Nariman Aga-Tagiyev

Nariman Aga-Tagiyev is an Application Security Architect with 20+ years of experience in software development. Since 2016, he has focused on advancing SSDLC maturity and building Application Security programs for international organizations. He is a core team member of OWASP SAMM, CEN/CENELEC EU CRA and ISO/IEC 27034 project working groups. He is also the founder of SecureHabits, helping industrial manufacturers prepare for the EU Cyber Resilience Act (CRA).

Dustin Lehr

Dustin Lehr is the Co-founder of Katilyst and an IANS faculty member. As a former software engineer and Cybersecurity leader, he now helps build developer-centric AppSec programs that motivate and incentivize security-minded behaviors. He is also the author of the Security Champion Program Success Guide and co-leads the League of Cyber Defense Champions global open discussion community.

Stanley Harris



Stanley is the CEO and Co-founder of Katilyst, where he leads initiatives to build and enhance Security Champion programs. With over 20 years of experience in organizational change management, he has successfully designed and launched dozens of security programs, fostering engaging and sustained security cultures. His background includes implementing agile and scrum methodologies at various high-profile companies, significantly improving project efficiency and collaboration. Stanley leverages his game design experiences to apply effective gamification techniques in professional settings.