ISC2 CHAPTER | EAST BAY

Eventbrite Registration

NINE LIVE LABS

The Secure AI Revolution

Friday March 13th, 2026 | 8:00 AM – 5:00 PM

Venue: Las Positas College, Livermore, CA

March 13th, 2026
8:00 AM to 5:00 PM
@Las Positas College

LAS POSITAS COLLEGE

2400 Campus Hill Drive
Livermore, CA 94551
Lot E, Bld. Exhibit & Lecture

Pricing—Early bird and partner codes available until February 28th. Your member login is your Promo Code.

- ISC2 East Bay Mem. $100/$125
- Student Member $45/$65
- Guest Registration – $145/$175
- Event Speakers, Sponsors, Volunteers—We send your ticket to you.

REGISTER NOW

https://www.eventbrite.com/e/nine-live-labs-the-secure-ai-revolution-a-practical-blueprint-tickets-1976091466772

To get member rates, Join today

isc2-eastbay-chapter.org

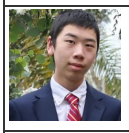
Keynote Speakers | Live Labs | Panel Discussion | Exhibitors

Breakfast | Lunch | Cake break

HIDDENLAYER

Malcolm Harkins, Chief Security and Trust Officer, HiddenLayer

Neil Daswani, Global Cybersecurity & AI Leader | Top 100 CISO | Firebolt Ventures

The Nine Live Labs	Sponsor, Speaker	Lab, Minimum OWASP LLM & Agentic AI Cov.
	HiddenLayer Jason Martin	Lab 1-1 RAG Rampage: Hands-On Prompt Injection and Defense in a Custom AI Bot
	Netskope Bob Gilbert	Lab 2-1 Poisoning the Well: Auditing Data and Preventing Leaks in Fine-Tuned Models
	Kratikal Pavan Kushwaha	Lab 3-1 The VIBE Check: Auditing AI-Generated Code for Security Flaws (SCA/IAST)
	Intezer Mitchem Boles	Lab 4-2 Genetic Analysis of AI Code: Rapid Triage and Malicious Code Family Identification
	Veria Labs Stephen Xu	Lab 5-2 Agentic Exploitation: Hijacking AI Tools in Real-Time: Practical API Hacking and De-
	Snyk Lea Tuizat and Jonathan Randall	Lab 6-2 Developer Security, SCA, and Supply Chain Risk
	Stellar Cyber Daniel Cheng	Lab 7-3 From Exploit to EDR: Correlating AI Application Attacks with Open XDR Response
	Mavs AI Amit Kharat	Lab 8-3 GenAI Runtime Security, and Data Security Posture Management (DSPM)
	Corelight Mike Henkelman	Lab 9-3 Network Forensics for AI Exfiltration and Model Theft

Full Attendance earns 8 CPE | Networking earns 5 CPE | Presentation and committee work earns up to 13 CPE

Platinum Sponsors

HiddenLayer (hiddenlayer.com) is the enterprise leader in Adversarial Machine Learning (AML) security. Their **MLSec Platform** provides a non-invasive, hardware-agnostic suite of security solutions designed to protect the integrity and intellectual property of AI models. By offering **Machine Learning Detection and Response (MLDR)**, HiddenLayer monitors model inputs and outputs in real-time to detect prompt injection, model extraction, and data poisoning—all without requiring access to an organization's raw data or proprietary algorithms. As a pioneer in the space, HiddenLayer helps enterprises secure their AI supply chain through **AI Bill of Materials (AIBOM)** generation, ensuring that every model deployed is verified, compliant, and resilient against evolving threats.

Netskope (netskope.com) is a global SASE leader that helps organizations apply **Zero Trust principles** and AI/ML innovations to protect data and defend against modern cyber threats. Through its **Netskope One** platform and **SkopeAI** capabilities, Netskope provides optimized visibility, real-time data protection, and advanced threat defense for users accessing cloud services, websites, and private applications from any location. As a key architect of the "Secure AI Revolution," Netskope enables enterprises to govern the entire AI development lifecycle—from auditing the data lineage used in RAG and model fine-tuning to managing **Data Security Posture Management (DSPM)**. By identifying over-privileged service accounts and securing the "Action Layer" where autonomous agents interact with sensitive data, Netskope ensures that AI-driven innovation remains secure, compliant, and resilient.

Stellar Cyber (stellarcyber.ai): Offers an Open XDR platform that unifies security operations across the entire attack surface. It ingests data from existing security tools, normalizes and enriches it, then applies proprietary AI/ML to automatically detect threats. The platform correlates high-fidelity alerts into incidents, accelerating investigation and enabling automated response actions. This approach enhances security operations center (SOC) effectiveness by providing comprehensive visibility, reducing noise, and improving analyst efficiency for rapid threat mitigation.

Intezer (intezer.com) is the leading **Autonomous SOC platform** designed to emulate the decision-making process of a human security analyst at machine scale. By leveraging proprietary **Genetic Malware Analysis**, Intezer automatically triages, investigates, and responds to every alert originating from an organization's existing security stack (EDR, SIEM, and Phishing reports). Unlike traditional automation that relies on rigid playbooks, Intezer's AI-driven platform identifies the "DNA" of code to distinguish between trusted software, known threats, and sophisticated new mutations. This allows security teams to automate over 90% of their Tier 1 and Tier 2 monitoring tasks, effectively eliminating alert fatigue while ensuring that critical incidents are triaged and remediated in seconds rather than hours.

Astrix Security (astrix.security) is the industry's first non-human identity (NHI) security platform, purpose-built to help enterprises secure the vast and often invisible web of service accounts, API keys, and OAuth tokens that power the modern automated enterprise. As organizations shift toward agentic AI and autonomous workflows, Astrix provides the only holistic solution for the entire NHI lifecycle—from automated discovery and risk assessment to real-time remediation. By securing SaaS-to-SaaS connectivity and managing the "Action Layer" where AI agents interact with corporate data, Astrix prevents unauthorized access and ensures operational continuity in an increasingly connected world.

Gold Sponsors

Corelight (corelight.com) is the pioneer and fastest-growing provider of Open Network Detection and Response (NDR), delivering a unique approach to cybersecurity risk centered on comprehensive network evidence. As the only solution powered by the dual open-source foundations of Zeek® and Suricata—now enhanced by GenAI—Corelight provides deep visibility into network traffic by transforming raw data into high-fidelity logs, metadata, and actionable insights. By equipping elite defenders at the world's most mission-critical enterprises and government agencies with this rich evidence, the platform enables rapid threat hunting, forensic analysis, and complete situational awareness across complex, distributed environments. Ultimately, Corelight helps security teams level up their defenses, accelerating investigations and dramatically reducing the time required to detect and neutralize sophisticated attacks and model theft.

Snyk (snyk.io) is the leader in developer security, providing an enterprise-grade, multi-layered platform powered by the DeepCode AI orchestration engine to secure every component of the modern software supply chain. By combining symbolic AI with machine learning, Snyk delivers real-time vulnerability scanning and automated fix suggestions across source code (SAST), open-source dependencies (SCA), container images, and infrastructure as code (IaC). Snyk's technical edge lies in its curated vulnerability database and its ability to integrate directly into the developer workflow, enabling security leaders to implement global risk policies while empowering engineering teams to remediate security debt without sacrificing deployment velocity. By bridging the gap between security and development, Snyk provides the scalability, visibility, and auditability required for large-scale digital transformations and secure AI adoption.

RevolutionCyber (revolutioncyber.com) is a boutique cybersecurity and resilience consulting firm that blends strategic advisory, cultural transformation, and technology enablement to redefine how organizations approach security. They focus on aligning security with core business outcomes, such as resilience, trust, and revenue generation, rather than treating it as a standalone technical function, offering services that enhance security culture and prepare for rapid incident response.

Sepio (sepiocyber.com) provides a Hardware Access Control (HAC) platform that offers visibility and control over all hardware assets utilizing physical layer fingerprinting. By using machine learning to analyze device behavior at the physical layer, Sepio identifies rogue devices and malicious hardware implants that bypass traditional security controls, ensuring the integrity of IT, OT, and IoT environments.

Exiger (exiger.com) is a global leader in AI-powered supply chain risk management, helping organizations illuminate and protect their extended enterprise and third-party ecosystems. Through its proprietary 1Exiger platform, the company provides real-insights into financial health, geopolitical exposure, and ESG risks, enabling proactive management of the complex dependencies that define modern global commerce.

Silver Sponsors

BalkanID (balkanid.com) provides modular, AI-assisted identity security and access governance (IGA) solutions designed to work with both connected and disconnected applications. Its platform streamlines critical tasks such as user access reviews, lifecycle automation with purpose-based just-in-time access, and identity security posture management (ISPM)—including IAM risk and RBAC analysis and an AI Copilot feature. By empowering organizations to enforce least privilege principles, BalkanID enables enterprises to efficiently manage complex identity risks at scale.

Happiest Minds Technologies (happiestminds.com) is an AI-led, digital engineering and "Mindful IT" company that delivers secure, scalable solutions spanning from chip to cloud. By integrating deep expertise in Gen AI with core capabilities in product engineering, cybersecurity, and automation, Happiest Minds helps enterprises across BFSI, Healthcare, and Hi-Tech fast-track their digital evolution. Their innovation-led strategy is supported by strategic partnerships with AWS and Microsoft, as well as a growing portfolio of proprietary platforms like Arttha and FuzionX.

Horizon3.ai (horizon3.ai) provides **NodeZero**, an autonomous penetration testing platform. It continuously assesses an organization's internal and external attack surface, automatically discovers exploitable weaknesses, and verifies vulnerabilities without human intervention. By rigorously emulating real-world attacker behaviors and techniques, NodeZero identifies critical attack pathways and provides clear, actionable remediation steps to proactively strengthen security posture and continuously validate an organization's defenses against evolving cyber threats, supporting a continuous security validation program.

Illumio [illumio.com]: Provides Zero Trust Segmentation to prevent the lateral movement of breaches across complex hybrid environments, including data centers, multi-cloud infrastructures, and endpoints. It meticulously visualizes application dependencies and communication flows, micro-segments networks down to individual workloads, and enforces granular, adaptive policies to contain attacks. This approach dramatically minimizes breach impact by reducing the attack surface and significantly enhancing an organization's overall cyber resilience and security posture.

Mavs AI (mavsai.com) delivers smart guardrails, intelligent policy control, and real-time visibility for every GenAI interaction. They address specific risks like PII and sensitive data shared in prompts, prompt injections compromising systems, and misuse by business users or rogue application users. Mavs AI closes the gap where innovation outpaces safety guardrails, enabling enterprises to innovate fearlessly and scale AI responsibly.

NetAlly (netally.com) offers portable network testing and analysis solutions essential for IT and cybersecurity professionals managing complex infrastructures. Its suite of tools provides deep visibility into both wired and wireless networks, enabling efficient troubleshooting of connectivity issues, precise validation of network performance, and verification of security configurations. This comprehensive approach helps ensure reliable network infrastructure, reduces downtime, and facilitates rapid issue resolution for enhanced operational stability and secure network operations.

Silver Sponsors

One Identity (oneidentity.com) delivers a unified identity security platform that provides comprehensive identity and access management (IAM) solutions across an organization's entire digital landscape. By bridging the gap between Identity Governance and Administration (IGA) for user lifecycle management, Privileged Access Management (PAM) for securing elevated accounts, and Access Management for secure authentication, One Identity provides a holistic, identity-centric approach to security. This unified platform helps organizations manage identities, govern access, and secure privileged accounts while streamlining identity lifecycles and enforcing least privilege principles. Ultimately, One Identity enables enterprises to improve their compliance posture and strengthen overall security across complex, hybrid IT environments.

Po Security (po.dev) is helping companies modernize PAM for multi-cloud and hybrid environments with the most agile way to ensure least-privileged, short-lived, and auditable production access for users, NHIs, and agents. Centralized governance, just-enough-privilege, and just-in-time controls deliver secure access to production, as simply and scalably as possible. Po's **Access Graph** and **Identity DNA** data layer make up the foundational architecture that powers privilege insights and access control across all identities and production resources, including the new class of AI-driven agentic workloads emerging in modern environments.

Redblock's Agentic AI (redblock.ai) automates identity and security workflows across disconnected apps — extending SailPoint and other identity systems for full coverage. It connects what Identity systems can't, eliminates CSVs and IT tickets, and automates actions safely with policy guardrails. The result: a smaller identity attack surface in days, not months. Manual workflows become autonomous, auditable actions.

StrongDM (strongdm.com), founded in 2015, offers a unified Zero Trust Access platform for managing and auditing access to all critical infrastructure, including databases, servers, Kubernetes clusters, and web applications. By connecting users securely without the need for traditional VPNs, StrongDM centralizes control over technical access and meticulously logs every session with precision for comprehensive auditing and compliance. The platform enforces granular, least-privilege access policies in real-time, significantly enhancing security posture while streamlining compliance workflows. Secure-by-design and boasting a 98% customer retention rate year-over-year, StrongDM is focused on making life easier and more operationally effective for technical experts by improving efficiency across complex, distributed environments.

Threatcop (threatcop.com) is an enterprise-grade cybersecurity awareness and simulation suite designed to tackle the most significant vulnerability in any organization: the human element. By combining AI-driven threat simulations—including phishing, vishing, and smishing—with real-time behavioral analytics, it empowers security leaders to identify, assess, and reduce people-centric risks while building a proactive "human firewall" against sophisticated social engineering. Threatcop's featured lab session will be conducted by its subsidiary, **Kratikal (kratikal.com)**. Kratikal is a leading provider of advanced cybersecurity solutions specializing in automated risk assessment, cloud security audits, and security simulation. Their platform enables organizations to identify and remediate vulnerabilities through comprehensive testing, combining automated technology with manual expertise to strengthen cyber resilience and ensure compliance with global security standards.

Veria Labs (verialabs.com) provides an AI-native offensive security platform designed for autonomous vulnerability discovery and exploitation. Founded by members of the #1 US competitive hacking team, Veria Labs builds specialized AI agents that integrate directly into Git repositories and CI/CD pipelines to analyze codebases continuously. These agents operate faster than human researchers, finding deep, complex vulnerabilities that traditional tools miss and generating real-world exploit PoCs to verify risk and eliminate false positives. By adapting to business logic and providing automated remediation, Veria Labs shifts offensive security left, enabling organizations to validate their security posture and secure critical vulnerabilities with high confidence and at machine speed.

ISC2 East Bay Chapter Board and Conference Committee


President, Conference Chair, Robin Basham


Treasurer, Irwin Cheng


Membership Chair, Nachiket Deshpande


Vice President,& Dir. Communications, Cyrus Haghighi


Secretary, Spence Gordon


Director Technology, Brian Payne


Director Operations, Karl Schneider


Director Sponsorship, Cory Brown


Director Programs, Abhishek Neelakanata


Director Marketing, Evan Tsai


Director Outreach, Dennis Esselsagoe


Director Awareness and Education, Nancy Mate'


Director Careers, Neha Dhage


Director Hospitality, Dawn Owna


Conference Coordinator (Shadow), Karina Lelaisromant


Speaker Liaison, Radek Urban


Technology Committee, Gary Dylina


Careers Committee, Bhawana Veenu


Conference Committee, Vendors, Daniel Cheng


Conference Committee, Vendors, Erica Cunningham


Conference Logistics Committee, Jim Gallagher


Conference Hospitality Committee, Katherine Greathouse


Conference Logistics Committee, Eliza Wong


Conference Hospitality Committee, Carmen Parrish


Technology Committee, Jim Danforth


Program Leader, Las Positas College
Jean O'Neil-Opipari


Cyber Program Leader, Las Positas College,
Anita Bhatia


Cyber Program Leader, Las Positas College,
Jeff Weichert

ISC2 is the world's leading member organization for cybersecurity professionals, driven by our vision of a safe and secure cyber world. Our nearly 675,000 members, candidates, and associates around the globe are a force for good, safeguarding the way we live. Our award-winning certifications – including cybersecurity's premier certification, the CISSP® – enable professionals to demonstrate their knowledge, skills, and abilities at every stage of their careers. ISC2 strengthens the cybersecurity profession's influence, diversity, and vitality through advocacy, expertise, and workforce empowerment, accelerating cyber safety and security in an interconnected world. Our charitable foundation, The Center for Cyber Safety and Education, helps create more access to cyber careers and educates those most vulnerable. Learn more and get involved at ISC2.org.

https://www.eventbrite.com/e/nine-live-labs-the-secure-ai-revolution-a-practical-blueprint-tickets-1976091466772

https://app.joinit.com/o/isc2-east-bay/

We could not provide this experience without the generosity of Las Positas College. Please give your thanks to our student volunteers, consider donating to the LPC Foundation.

We also invite everyone attending to join at least one other professional organization because we are stronger together.

Please ask us about partner member codes.