

**MARCH 24-26, 2025 | EXPO TEL AVIV**

## MARCH 24

**THE LAUNCH OF CYBERTECH GLOBAL TEL AVIV: GLOBAL FORUMS, SPECIAL THINK TANKS, AND SEMINARS**

**Identity Think Tank: The Exclusive Identity Forum**

**The CISOs-Founders Meeting**

**AI Special Seminar**

**Meet the Experts: Exclusive One-on-One Meetings Between a Panel of Experts and Promising Startups**

## MARCH 25

**9:00-18:00 | PLENARY HALL**

9:00-12:30	<p><b>OPENING PLENARY</b></p> <p>Top-level keynotes and presentations by leading government, industry, and academia speakers from around the globe</p>
12:30-13:00	<p><b>SPECIAL DISCUSSION AMONG CISOs, FOUNDERS, AND INVESTORS</b></p>
13:00-14:00	<p><b>LUNCH BREAK AND EXHIBITION</b></p>
14:00-14:35	<p><b>NATIONAL AND GLOBAL CYBER CHALLENGES: ADVANCING CYBERSECURITY THROUGH INTERNATIONAL COLLABORATION IN CYBER</b></p>
14:35-15:45	<p><b>TECH STAGE</b></p> <p><b>AI FOR CYBER AND CYBER FOR AI</b></p> <p>The value of AI in cybersecurity</p> <p>Proactive protection: How to utilize AI systems for better cybersecurity</p> <p>The race between attackers and defenders</p> <p>AI-based cybersecurity posture management systems</p> <p>AI you can trust: Protection of AI systems</p> <p>Purpose-built AI for secure development</p> <p>AI-powered attacks - AI use by adversaries</p>
15:45-17:00	<p><b>CLOUD ADVANCED CYBERSECURITY SOLUTIONS</b></p> <p>The journey to secure the hybrid cloud</p> <p>National clouds: Laws, regulations, compliance, and standards</p> <p>The attacker's angle: Current and future trends on cloud attacks</p> <p>Data breach prediction</p> <p>Continuous exposure reduction for the hybrid attack surface</p> <p>Less than Zero Trust: AI-powered real-time authentication and activity monitoring</p> <p>DevSecOps and security automation</p> <p>SaaS security services</p> <p>Protecting data security posture management (DSPM)</p>
17:00-18:00	<p><b>CYBERSECURITY CHALLENGES AND OPPORTUNITIES IN THE QUANTUM ERA - PREPARING FOR A SECURE FUTURE IN THE QUANTUM AGE</b></p> <p>Cyber opportunities in the Quantum Age</p> <p>Risks and challenges posed by quantum computing</p> <p>Quantum-powered cyber attacks by malicious actors</p> <p>Transitioning to quantum-safe encryption</p> <p>Global collaboration on quantum security standards</p>
18:00-20:00	<p><b>BEER AND BUSINESS: FORMAL INTERNATIONAL RECEPTION</b></p> <p><b>*FOLLOWING THE END OF THE CONFERENCE* (BY INVITATION ONLY)</b></p>



# CYBERTECH GLOBAL TEL AVIV 2025

## MARCH 25

11:00-17:00 | SPECIAL SEMINARS

HALL B	HALL C	HALL D
11:00-13:00 <b>Special Simulation Event: Cyber and EMP Attack Global Crisis Management</b>	14:00-15:00 <b>The Secrets of Unit 8200</b> Special Discussion by the 8200 Alumni Association	15:00-17:00 <b>Invest in the Best</b> The main exclusive meeting between selected startups and leading investors
14:00-15:30 <b>An Ocean of Risks: The Global Forum for Maritime Cybersecurity</b>	15:00-16:00 <b>Creating New Tech and Innovation Hubs Globally</b>	
15:30-17:00 <b>Aviation Cybersecurity: State-of-the-Art Threats on the Horizon</b>	16:00-17:00 <b>Inclusion of Diverse and Competent Talents for the Cyber Industry</b>	

## MARCH 26

9:00-18:00 | PLenary HALL

9:00-12:00	<b>TEL AVIV TECH WEEK STAGE</b> <b>THE OFFICIAL OPENING OF THE SPARKS INNOVATION SUMMIT IN CONJUNCTION WITH CYBERTECH</b> Top-level keynotes and presentations by leading government, industry, and academia speakers from around the globe.
12:00-12:30	<b>CYBERSECURITY IN FINANCIAL SERVICES</b>
12:30-13:00	<b>WHAT WILL BE THE NEXT BIG THING IN CYBER? THE MAIN INVESTMENT DISCUSSION</b>
13:00-14:00	<b>LUNCH BREAK AND EXHIBITION</b>
14:00-18:00	<b>THE TEL AVIV SPARKS INNOVATION SUMMIT STAGE</b> For more information, visit <a href="http://tlvsparks.com">tlvsparks.com</a>

## MARCH 26

14:00-18:00 | THE CYBERTECH STAGE - HALL B

	<b>HACKING THE TRUTH: NEW WORLD OF FAKE AND TRUTH</b> Misinformation, fake news, and manipulation of social discourse Deepfake, identity theft, fake accounts, and other social media threats GenAI content and image generators as emerging tools in the arsenal of malicious actors Social engineering attacks Mistrust in real texts, images, and videos
	<b>CYBER WARFARE: NATIONS UNDER ATTACK</b> Lessons Learned from wars in Ukraine, Gaza and around the world Case study analysis of major attacks on nation-states Advanced Persistent Threats (APTs) and state-sponsored hacking groups Corporate assistance provided to states in times of crisis Cyber crisis management



**MARCH 26**

**14:00-18:00 | THE CYBERTECH STAGE - HALL B**

	<p><b>CYBER INTELLIGENCE OPERATIONS FOR NATIONAL AND INTERNATIONAL SECURITY</b></p> <ul style="list-style-type: none"><li>Intelligence agencies: Proactive response role in cyber threats</li><li>Challenges of cyber intelligence operations under international law</li><li>Future innovations that are changing the cyber intelligence landscape</li><li>Lessons learned from over a decade in OSINT</li><li>Dark web and dark net cyber intelligence collection</li><li>Cyber HUMINT: Engaging with threat actors for intelligence gathering</li><li>International collaboration for national and international security</li></ul>
	<p><b>PROTECTING CRITICAL INFRASTRUCTURE (CI) FROM CYBERATTACKS</b></p> <ul style="list-style-type: none"><li>Rapid digital transformation of CI and new cybersecurity risks</li><li>Available approaches and tools to support CI protection</li><li>Lessons and recommendations in the domain of cyber capacity-building</li><li>Business continuity, emergency preparedness, and cyber resilience for critical assets</li><li>Enhancing cybersecurity in critical sectors: Regulations, policies, and strategic approaches<ul style="list-style-type: none"><li>Multilayer defense for critical entities</li><li>Managing a cyber-attack – dos and don'ts</li><li>Disaster Recovery</li><li>SOCs</li></ul></li></ul>
	<p><b>SOFTWARE SUPPLY CHAIN SECURITY</b></p> <ul style="list-style-type: none"><li>Lessons learned from major latest attacks</li><li>Key cyber supply chain risks: Software aspects</li><li>Steps to prevent supply chain attacks or to minimize their impact</li><li>Managing cyber risk in the supply chain<ul style="list-style-type: none"><li>Cybersecurity for retail</li><li>Network detection and response (NDR)</li></ul></li></ul>
	<p><b>PRIVATE-PUBLIC PARTNERSHIPS: A STRATEGY FOR CREATING A ROBUST CYBERSECURITY ARRAY</b></p> <ul style="list-style-type: none"><li>Collaboration between governments and the private sector<ul style="list-style-type: none"><li>The power of industry giants</li></ul></li><li>Overcoming challenges for establishing successful partnerships<ul style="list-style-type: none"><li>Regulation and legislation</li></ul></li><li>Public and private investments in security technologies<ul style="list-style-type: none"><li>Joint cybersecurity operations</li><li>Case studies of successful PPPs</li></ul></li></ul>