

RSAC | 2026
Conference

FROM SINGAPORE TO THE WORLD

Trusted Secure Innovation



Co-organized by:



SGTECH
WHERE TECH MEETS

Featuring:



 **AxisNow**

 **Cyber Sierra**

digiDations
Continuously Validate Continuously Secure

 **PROTOS LABS**

PQC Be Quantum Ready

 **SCANTIST**

 **StrongKeep**

CONTENTS

03 TIG Centre

05 Agile Momentum

06 AxisNow

07 Cyber Sierra

08 digiDations

09 pQCee

10 Protos Labs

11 Scantist

12 StrongKeep



CyberSG TIG Collaboration Center

TIG Center: Powering Singapore's Cybersecurity Innovation for the World

As cyber threats grow in scale and sophistication, so does the need for closer collaboration between countries and organisations to create trusted, scalable solutions.

CyberSG Talent, Innovation and Growth (TIG) Collaboration Center is Singapore's national platform for cybersecurity ecosystem development, uniting government, academia, industry, and innovators to speed up turning ideas into tangible real-world results.

Established by the Cyber Security Agency of Singapore (CSA) in partnership with National University of Singapore (NUS), the TIG Center serves as a central hub for building capabilities, catalyzing innovation, and enabling global growth across Singapore's cybersecurity landscape.

A Unified Engine for Talent, Innovation, and Growth

The Center is built on three integrated pillars that collectively strengthen Singapore's position as a leading cybersecurity hub:

Talent

Developing a future-ready cybersecurity workforce through industry-aligned programs, partnerships, and continuous upskilling, from students to experienced professionals.

Innovation

Accelerating the commercialization of cybersecurity technologies by connecting startups, researchers, and enterprises to solve real-world challenges.

Growth

Supporting companies in scaling beyond Singapore through market access, global partnerships, and internationalization initiatives.

Driving Innovation That Matters

TIG Center enables co-innovation between industry and the research community to address pressing cybersecurity challenges. The flagship initiatives include:

- **CyberCall:** A national innovation call that challenges companies to develop solutions addressing real-world cybersecurity needs
- **CyberBoost:** A structured program supporting startups and scale-ups through mentorship, capability development, and access to market.

These programs are designed to move innovation beyond ideas, helping companies validate solutions, secure partnerships, and achieve commercial traction. Building on Singapore's broader innovation ecosystem, including the NUS Enterprise and BLOCK71 networks, TIG Center enables companies to tap into global nodes for development and scaling. Through these efforts, it promotes collaboration that bridges research, commercialization, and market expansion.

Connecting Singapore to the World

TIG Center plays a critical role in positioning Singapore as a launchpad for global cybersecurity innovation. Through initiatives such as **CyberGrowth**, companies are supported in expanding into international markets, building strategic partnerships, and navigating global business environments.

The Center also leads international engagements, including the Singapore Pavilion at RSAC, where Singapore-based companies showcase cutting-edge solutions to global audiences, from AI-driven security to post-quantum cryptography.

These efforts strengthen Singapore's reputation as a trusted source of cybersecurity innovation and create meaningful opportunities for collaboration with enterprises, investors, and governments worldwide.

Building a Trusted Cybersecurity Future

At its core, TIG Center exists to ensure that innovation translates into real-world outcomes.

By aligning ecosystem partners and supporting the full lifecycle of cybersecurity development — from talent cultivation to global market expansion — TIG Center enables Singapore's cybersecurity capabilities to scale with confidence, credibility, and impact.

From Singapore to the world, TIG is shaping the future of trusted, secure innovation.



Explore our companies instantly

rsa.cybersg.sg

Meet Us at RSAC



Willis Lim
Executive Director



Daniel Ong
Program Manager

✉ cybergrowth@cybersg.sg



in LinkedIn
tig.cybersg.sg

📍 Meet Us at Singapore Pavilion, S-1945

About The Company

Agile Momentum is a cybersecurity company focused on **behavioral risk deterrence** — protecting sensitive information at the moment human decisions are made. Most security tools monitor data in motion or at rest. But once sensitive information appears on a screen, it can leave instantly through a smartphone camera or simple human error.

Agile Momentum addresses this overlooked gap by making security visible where people actually interact with data — directly on the screen. Grounded in behavioral science, the company designs systems that influence decisions in real time, helping organizations reduce accidental data exposure and build a stronger security culture at scale.

The Solution

AgileMark is a dynamic screen watermarking solution designed to stop one of the fastest-growing data leak paths: phone cameras capturing sensitive screens.

Traditional controls lose visibility once information reaches the screen. AgileMark restores accountability by placing dynamic watermarks and behavioral cues directly where the risk occurs.

These visible signals deter photo-snapping, reduce accidental exposure, and guide employees before risky actions happen.

Rather than simply monitoring activity, AgileMark changes the conditions in which decisions are made — turning the screen itself into an active security control. The result is deterrence before incidents occur, clear attribution when they do, and a workforce guided to make safer decisions in real time.

Meet Us at RSAC



Ron Wee
Partner

✉ ron.wee@agilemark.io



in LinkedIn
agilemark.io |
agilemark.com (Website 2.0)

📍 Meet Us at Singapore Pavilion,
S-1945

About The Company

AxisNow is a Singapore-based technology company transforming how organizations deliver and secure applications at the network edge. As businesses expand across multiple clouds, mobile platforms, and global markets, traditional CDN and cloud architectures struggle to balance performance, security, and cost.

AxisNow provides a cloud-agnostic multi-cloud edge platform that gives organizations greater control, flexibility, and resilience. By decoupling edge deployment from proprietary vendor networks, AxisNow helps enterprises avoid lock-in, simplify operations, and maintain sovereignty over their data and security policies.

The Solution

AxisNow delivers a unified multi-cloud edge control layer that simplifies private CDN deployment, multi-CDN orchestration, and edge-level security.

Private Edge Platform

Enables organisations to deploy and manage self-hosted edge nodes on their own infrastructure, providing direct control over performance, traffic routing, and security policies.

Multi-Cloud Edge Orchestration

Centralizes management of multiple CDNs under one interface, allowing intelligent traffic steering, automated failover, and real-time visibility across providers.

SASE for Mobile Applications

Extends Zero Trust and SASE principles directly into native mobile applications, embedding security into application delivery without additional infrastructure complexity.

Meet Us at RSAC



Andy Ong
Co-Founder and CEO
✉ andy@axisnow.io



Gigi Tuang
Product Manager
✉ gigi@axisnow.io



James Hu
Co-Founder
✉ james@axisnow.io



in LinkedIn
axisnow.io

📍 Meet Us at Singapore Pavilion, S-1945

About The Company

Cyber Sierra is an AI-powered cybersecurity platform that helps enterprise security and compliance teams scale their expertise across cyber operations, risk management, and audit readiness. As organizations face increasing regulatory demands, operational complexity, and talent shortages, Cyber Sierra enables teams to maintain high standards of security and governance without expanding headcount or relying on manual processes.

Founded by experienced cybersecurity practitioners, Cyber Sierra combines advanced AI with enterprise-grade governance to support secure and controlled deployment within complex environments. The platform is designed to strengthen institutional capability while preserving trust, traceability, and accountability.

The Solution

At the core of Cyber Sierra's offering is the **Cyber Sierra AI Analysts Platform**, a governed, multi-agent AI infrastructure built for cyber operations, governance, risk, and compliance.

Cyber Sierra's AI Analysts work across trusted internal security systems to generate verified, audit-ready outputs such as compliance reports, risk assessments, control monitoring summaries, incident postmortems, and board-level materials. Tasks that traditionally take weeks of manual effort can be completed in minutes with improved consistency and accuracy.

Unlike traditional automation tools that rely on rigid playbooks, Cyber Sierra enables adaptive, secure execution of complex workflows while maintaining enterprise-grade oversight. Organizations can deploy AI flexibly across different architectures and compliance environments, ensuring control without sacrificing speed.

Cyber Sierra has been recognised for its innovation and impact, including the CRPO Translation and Innovation Award 2025, the AI Trailblazer Innovation Award 2024 by Smart Nation Singapore in collaboration with Google, and inclusion in the Gartner Hype Cycle for Cyber Risk Management 2024 under Cyber GRC and Continuous Controls Monitoring.

By transforming trusted internal security signals into reliable, decision-ready outputs, Cyber Sierra enables organizations to operate more efficiently while reserving human judgment for the decisions that matter most.

Meet Us at RSAC



Pramodh Rai
Co-Founder

✉ pramodh@cybersierra.co



in LinkedIn
🌐 cybersierra.co
✕ @sierra_cyber
▶ @Cyber_Sierra

📍 Meet Us at Singapore Pavilion,
S-1945

About The Company

digiDations is an AI innovator building toward an Autonomous Digital Workforce, intelligent systems designed to continuously perform complex digital operations traditionally handled by human teams. Its first application focuses on cybersecurity, where AI is used to validate and strengthen organizational defenses through Adversarial Exposure Validation. By combining artificial intelligence with adversary-informed threat intelligence, digiDations enables organizations to continuously test their security posture and identify exploitable gaps before attackers do.

The company is supported by the CRPO Translation and Innovation Grant Series 2 and has achieved ISO 27001 certification. Through collaboration with CyberSG TIG and CRPO, digiDations contributes to strengthening Singapore's cybersecurity ecosystem and advancing proactive security validation practices.

The Solution

digiDations delivers its capabilities through an integrated portfolio of AI-driven technologies designed to help organizations continuously understand and validate their cyber resilience. This portfolio supports a comprehensive Adversarial Exposure Validation approach that enables organizations to discover exposures, simulate realistic attacks, and verify the effectiveness of their security defenses.

The **HELIOS External Attack Surface Management Platform** provides continuous visibility into an organization's internet-facing assets, identifying domains, subdomains, IP addresses, services, and exposed applications. Using AI-driven analysis, HELIOS helps security teams detect hidden assets, monitor exposure changes, and identify risks that adversaries could exploit.

The **APOLLO Continuous Automated Red Teaming Platform** executes realistic multi-stage adversarial campaigns that emulate real attacker behavior, including phishing, exploitation, lateral movement, and data exfiltration. These automated simulations help organizations understand potential attack paths and continuously assess how their defenses perform against evolving threats.

The **ORION Threat Intelligence Platform** provides the intelligence foundation of the ecosystem by continuously analyzing global threat data, vulnerabilities, indicators of compromise, and adversary behavior. This intelligence enriches attack scenarios, prioritizes emerging risks, and ensures validation activities remain aligned with the latest real-world threats.

At the core of the portfolio is the **ATLAS Security Validation Platform**, which continuously tests how security controls, detection systems, and response processes perform against realistic adversarial techniques. By safely simulating attack behavior within live environments, ATLAS identifies exploitable gaps, detection weaknesses, and response inefficiencies, delivering clear, prioritized insights that enable organizations to strengthen their security posture and focus remediation efforts where they matter most.

Powering the portfolio is **TARA (Threat Analysis and Research Assistant) AI**, digiDations' intelligent interaction layer that enables users to work with the platform using natural language. Rather than navigating complex workflows, security teams can describe the validation objectives, attack scenarios, or intelligence queries they want to perform, and TARA AI translates those requests into automated tasks, simulations, and analytical outputs.

Meet Us at RSAC



Tim Nan
Co-Founder & CEO

✉ tim@digidations.com



Zhengzi Xu
Co-Founder & Chief Scientist

✉ zhengzi.xu@digidations.com



in LinkedIn
🌐 digidations.com

📍 Meet Us at Singapore Pavilion,
S-1945

About The Company

pQCee is a Singapore-based quantum cybersecurity company focused on protecting the digital economy from the emerging risks of quantum computing. As advances in quantum technology threaten to weaken traditional cryptographic systems, pQCee develops post-quantum security solutions that help organisations future-proof their applications, communications, and infrastructure.

The company addresses a growing global concern known as “harvest-now-decrypt-later,” where encrypted data is collected today with the intention of decrypting it once quantum capabilities mature. pQCee supports governments and enterprises in preparing for this transition by strengthening cryptographic resilience while enabling a practical path toward quantum-ready security.

The Solution

pQCee provides a comprehensive portfolio of post-quantum products designed for real-world deployment and interoperability.

- **SafeGuard** protects data assets and communications against harvest-now-decrypt-later risks using post-quantum encryption.
- **QKDLite** is a quantum key management middleware that connects existing enterprise and cloud infrastructure to quantum technologies without major architectural changes.
- **QulCScript** is a real-time quantum simulator used by universities and research institutions for teaching, research and experimentation.
- **inoQulate** delivers post-quantum public key infrastructure and digital signing to secure identities, certificates, and transactions against future quantum threats.
- **PacketQC** is a postquantum discovery, inventory and governance tool to help organizations track their quantum-readiness.
- **PQ Web 3** applies post-quantum cryptography to blockchain systems, securing Web3 transactions and smart contracts against future quantum attacks.

pQCee’s capabilities are reinforced through collaborations with Thales on quantum key distribution and encryption initiatives, as well as partnerships with Netrust on quantum-safe document signing services. These engagements demonstrate pQCee’s ability to translate advanced cryptographic research into deployable enterprise solutions.

By focusing on interoperability, gradual adoption, and operational readiness, pQCee helps organisations strengthen security today while preparing for the long-term impact of quantum computing.

Meet Us at RSAC



Teik Guan Tan
CEO & Co-Founder

✉ teikguan@pqcee.com



Chay Hiah Loh
CFO & Co-Founder

✉ chayhiah@pqcee.com



in LinkedIn
🌐 pqcee.com

📍 Meet Us at Singapore Pavilion,
S-1945



About The Company

Protos Labs is a Singapore-based Cyber AI company tackling one of today's most urgent cybersecurity challenges: the growing gap between increasingly automated attackers and overstretched human security teams. As threats scale in speed and complexity, organizations face analyst shortages, rising alert volumes, and pressure to make faster, more consistent decisions.

Protos Labs introduces a new model for cyber defense by deploying reasoning-based AI agents that work alongside human analysts. Rather than replacing people, the company focuses on scaling human expertise through intelligent automation.

The Solution

At the core of its platform is **Protos AI**, an AI agent system designed specifically for Cyber Threat Intelligence. Protos AI integrates directly with existing security tools and threat feeds, enabling organizations to extract more value from their current technology investments without replacing their infrastructure.

Unlike traditional rule-based automation, Protos AI performs open-ended investigations. Its agents collect data, correlate signals across multiple sources, form hypotheses, and recommend mitigation actions by reasoning through complex and evolving threat scenarios. The platform mirrors how experienced analysts think, allowing security teams to move beyond static workflows and fragmented tools. It is also designed to be LLM-agnostic, giving enterprises flexibility in model deployment while avoiding vendor lock-in.

By scaling analyst reasoning through AI, Protos Labs enables organizations to respond to threats up to 15 times faster, reduce operational costs, and free skilled analysts to focus on strategic, high-impact work. The company has validated its approach through paid proof-of-concepts with Fortune 1000 companies and Information Sharing and Analysis Centers, positioning itself as a pioneer in reasoning-based AI agents for cyber intelligence.

Through this human-plus-AI approach, Protos Labs helps enterprises strengthen cyber resilience while maintaining control, flexibility, and institutional knowledge in an increasingly complex threat landscape.

Meet Us at RSAC



Joel Lee
CEO & Co-Founder

✉ joel_lee@protoslabs.sg



Simeon Tan
Co-Founder and CTO

✉ simeon_tan@protoslabs.sg



in LinkedIn
🌐 protoslabs.io

📍 Meet Us at Singapore Pavilion,
S-1945



About The Company

Scantist is an AI-driven application and AI security company that delivers autonomous, continuous penetration testing and software supply chain protection for modern development environments. Spun off from Nanyang Technological University, Scantist was founded to address the limitations of traditional security testing, which is manual, periodic, and often unable to keep pace with rapid software development and emerging AI risks.

By combining automation with intelligent validation, Scantist enables organizations to move from reactive testing to continuous security assurance across both software and AI systems.

The Solution

Scantist provides a unified security platform that delivers end-to-end protection across the software and AI lifecycle.

Its flagship product, **PAIStrike**, uses autonomous, multi-agent AI to simulate real-world attackers and perform continuous penetration testing without manual intervention. These AI agents conduct reconnaissance, exploit validation, and reporting to identify real, exploitable vulnerabilities, helping teams prioritize remediation and reduce false positives.

AppDefender strengthens DevSecOps and software supply chain security through SCA, SAST, and SBOM capabilities, identifying vulnerabilities in code, binaries, and dependencies. **AIDefender** extends protection to AI and LLM systems, addressing risks such as prompt injection, model misuse, and AI-specific attack vectors.

The platform integrates into CI/CD pipelines, supporting agile development while maintaining continuous compliance with standards such as GDPR and ISO/IEC 27001.

Scantist is ISO/IEC 27001:2022 certified and has received multiple industry recognitions, including the Google -EDB AI Trailblazer Transformation Award 2024 and the IMDA TechBlazer Award for Most Promising Innovation 2023. Through autonomous security validation, Scantist enables organizations to innovate confidently while maintaining trust and resilience

Meet Us at RSAC



Charles Huang
COO

✉ charlesh@scantist.com



in LinkedIn
🌐 scantist.com
✂ @ScantistAI

📍 Meet Us at Singapore Pavilion,
S-1945



About The Company

StrongKeep provides cybersecurity for the 99% of companies excluded by the cyber industry: Simple, Affordable, Comprehensive.

Most cybersecurity tools are designed for large enterprises with dedicated security teams. Small and mid-sized businesses are left choosing between fragmented tools that require technical expertise, or expensive consultant-led services.

StrongKeep productizes cybersecurity into a self-serve platform designed specifically for SMBs. By combining agentic-led automation, integrated security tools, and compliance workflows, organisations can deploy meaningful cybersecurity protections without needing in-house security expertise.

The Solution

StrongKeep provides an integrated, easy-to-use platform that bundles essential cybersecurity protections and compliance readiness into one solution.

The Protection Plan delivers foundational capabilities including endpoint security, DNS filtering, cybersecurity awareness training, phishing simulations, password management, and incident preparedness. It is designed for rapid deployment, requiring minimal setup and no specialist knowledge, allowing small teams to materially reduce cyber risk without operational burden.

The Compliance Plan guides organizations toward baseline certifications such as Cyber Essentials. It includes structured workflows, reminders, evidence tracking, and audit logs to support both certification and ongoing compliance. This helps SMEs demonstrate cyber hygiene and meet regulatory or customer requirements without hiring dedicated security staff.

By focusing on practical, “good-enough” cybersecurity, StrongKeep reduces reliance on consultants and eliminates the need to manage multiple vendors. Clear, predictable pricing aligns with SME budgets while ensuring coverage across technology, human risk, and compliance readiness.

Supported by an R&D partnership with A*STAR under CRPO’s Translation and Innovation Grant, StrongKeep continues to enhance its platform with scalable vCISO capabilities, reinforcing its mission to deliver effective cybersecurity outcomes for organizations without a CISO.

Meet Us at RSAC



Gaurav Keerthi
CEO

✉ gaurav@strongkeep.com



Zaishao Cheng
Partner & COO

✉ zaishao@strongkeep.com



in LinkedIn
🌐 strongkeep.com

📍 Meet Us at Singapore Pavilion,
S-1945

**Connect with the leading edge of
cybersecurity innovation at**

**Singapore Pavilion
Booth S-1945**

