INTERQUEST

Welcome

Digital Defence Forum 2025
AI in Business & Security

Keynote Presentation

”How to implement AI within your infrastructure as on prem and in the cloud? Tech & Cyber Lead, Harry Vidler, is joined by Dr Henk Jan Jansen to discuss how AI is going to change and revolutionise the future for Tech & Security.”

Harry Vidler
Managing Consultant InterQuest Group
Harry.Vidler@interquestgroup.com

Dr. Henk Jan Jansen
Founder & CEO
HJ Interim
Dr.Henkjan.jansen@hjinterim.net

INTERQUEST

Main Topics

1. Introduction Who I am
2. Top Cybersecurity & Innovation Challenges in 2025
3. AI – The Double-Edged Sword
4. What are the AI risks within Business
5. AI-Driven Cybersecurity Solutions & Key Benefits

Break

6. Emerging Technology Trends
7. AI & Cloud Security Strategies
8. Cybersecurity Talent Development
9. Key Considerations
10. Benefits of Artificial Intelligence (AI)
11. Some thoughts……

INTERQUEST

Who I am

Dr. Henk Jan Jansen Security Tech Enthusiast, Bridging the Gap Between Ideas, Execution & Innovating for a Better Tomorrow, has over 35 years of experience within Technology and Information Security, having worked across multiple industries including the Military, Automotive Industry, Healthcare, Federal Government, and Finance Industries as an Information Security Leader & Senior Program Manager.

Dr. Henk Jan Jansen is at the forefront of AI adoption and research within the Tech & InfoSec worlds, regularly presenting at key industry events and sharing his insights and research to ever improve our adoption and future with AI.

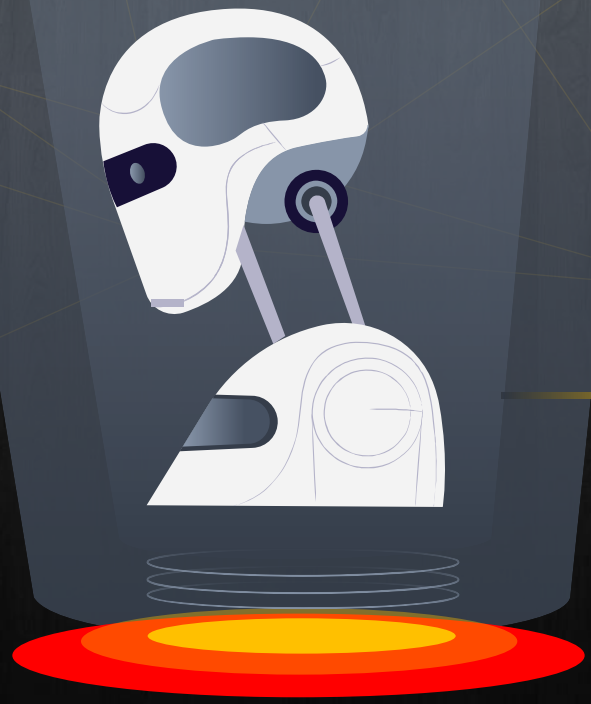
- Founder & CEO of HJ Interim since 1987
- Cybersecurity & digital transformation leader with 30+ years of experience
- Expert in cybersecurity, compliance, digital transformation & (Inter)National Law.
- Built and led Global Security Operations Centers (SOCs)
- Enhancing cyber resilience across multiple regions.
- Managed large-scale compliance programs
- Expertise in DORA, AVG, NIS2, ISO 2700x, BIO, DNB Good Practice, EBA Guidelines, Nen & Nen-EN, PRA, ESMA Regulation and NESA frameworks.
- Strategic advisor on balancing risk and innovation
- Helping businesses align security with growth.

INTERQUEST

But enough talk let's start with this event

INTERQUEST

Digital Defence Forum 2025
AI in Business & Security



Dr. Ir. Henk Jan Jansen

INTERQUEST

Top Cybersecurity & Innovation Challenges in 2025

- AI-powered cyber threats, including deepfake phishing and automated exploits
- Supply chain vulnerabilities: 60% of breaches now originate from third-party vendors (Gartner)
- Quantum computing threats: Encryption risks emerging

66% of CISOs believe cybersecurity budgets are too reactive (SC Media, 2025).

INTERQUEST

AI – The Double-Edged Sword

- AI-powered cybersecurity: Real-time threat detection, predictive security
- AI-driven cyberattacks: Deepfake phishing, AI- generated malware, and automated exploits

AI-driven phishing attacks have increased dramatically since 2022:

•1,265% increase since late 2022: This surge coincided with the mainstream adoption of AI tools like ChatGPT, enabling attackers to craft highly personalized and convincing phishing emails at scale.

•1,000% increase between 2022 and 2024: This growth reflects the widespread adoption of generative AI for phishing campaigns targeting user credentials.

•138% increase in phishing sites from 2022 to 2023: The rise in detected phishing sites highlights how generative AI has intensified cyber threats.

INTERQUEST

What are the AI risks within Business

- Automation-spurred job loss
- Bias and discrimination risks
- Privacy violations
- Cybersecurity threats
- Intellectual property infringement
- Financial crises caused by AI algorithms
- Market volatility
- Environmental harms
- Lack of accountability
- Overreliance on AI leading to reduced human influence
- Uncontrollable self-aware AI
- Increased criminal activity (e.g., deepfakes, voice cloning)
- Broader economic and political instability
- Errors magnified by AI transaction volume
- Skills gap in managing AI systems

INTERQUEST

AI-Driven Cybersecurity Solutions & Key Benefits

"Some tools"

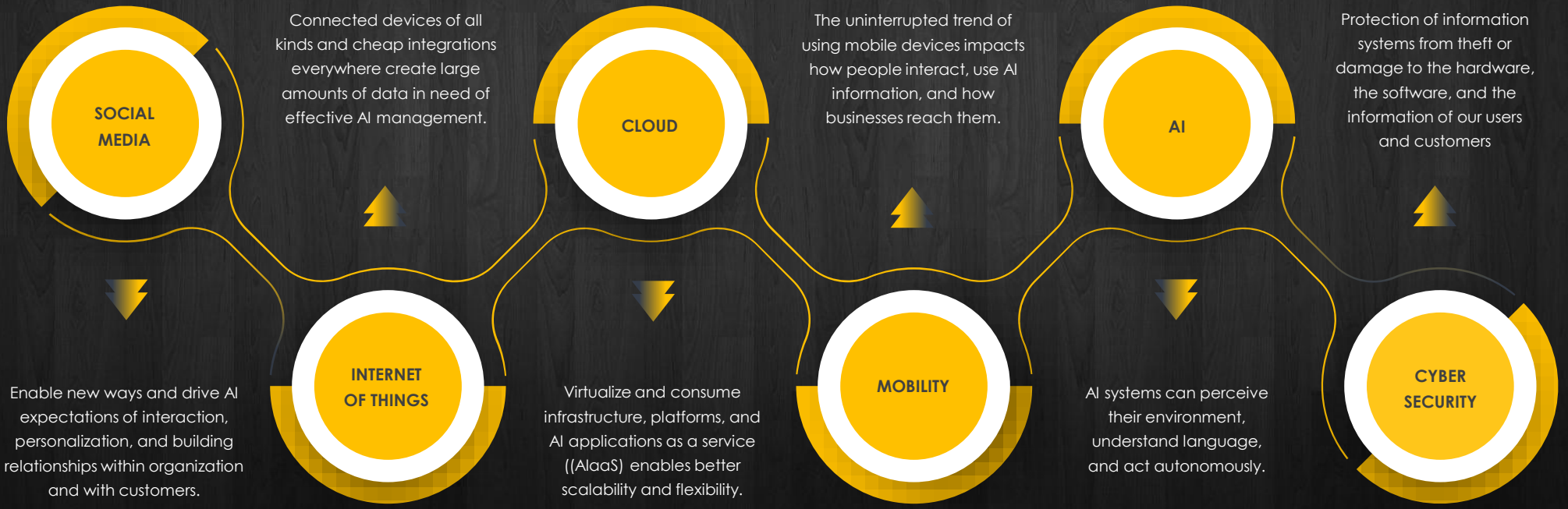
- Proactive Threat Detection: AI-powered systems can analyze vast datasets to uncover hidden patterns and identify risks before they escalate
- Real-Time Response: Automated responses help mitigate threats instantly, reducing the window of opportunity for attackers
- Adaptive Defense: Machine learning enables AI systems to evolve alongside new attack methods, ensuring defenses stay current
- Streamlined Operations: By minimizing false positives and automating repetitive tasks, AI allows security analysts to focus on high-priority investigations
- Microsoft Security Copilot: Leverages a specialized language model integrated with Microsoft's vast security ecosystem, processing over 65 trillion daily signals
- SentinelOne: Offers comprehensive threat detection, analysis, and response through its Purple AI platform, excelling in automated threat detection and real-time response automation
- Google SecOps: Provides a powerful suite of tools for improved threat detection, investigation, and response, featuring an AI-powered detection engine and natural language processing capabilities.
- Darktrace: Utilizes Self-Learning AI and Autonomous Response features to detect subtle anomalies and neutralize in-progress attacks without disrupting business operations
- SOCRadar: Enhances threat intelligence services by leveraging AI for efficient threat hunting and dark web monitoring, reducing false positive alerts by up to 90%
- Customized Threat Intelligence: AI systems are increasingly able to tailor insights based on an organization's specific industry, geography, and operational needs
- Enhanced Vulnerability Management: AI-driven platforms offer detailed reports on vulnerabilities, including their lifecycle, exploitation risks, and mitigation strategies
- Dark Web Monitoring: Advanced AI systems can dive into hidden online forums and marketplaces to uncover potential threats and data leaks
- Integrated Security Ecosystems: AI-powered platforms are being designed to seamlessly integrate with existing security tools like SIEM and SOAR, enhancing overall incident response capabilities

INTERQUEST

Let’s have a break for 15 minutes

INTERQUEST

Emerging Technology Trends



At the moment the financial industry is also very busy to implement AI within their infrastructure.

INTERQUEST

AI & Cloud Security Strategies

- Zero Trust Security Model

Adopting a Zero Trust approach is fundamental to modern cloud security. This model treats every access request as untrusted, requiring verification of user identity and device health before granting access to resources.

- Enhanced Access and Identity Management

Implementing strong Identity and Access Management (IAM) practices is essential.

- Data Encryption

Encryption is crucial for protecting data both in transit and at rest. Strong encryption algorithms, such as AES-256, should be used for sensitive data, along with regular key management practices.

- Continuous Monitoring and Threat Detection

Cloud environments should be continuously monitored for suspicious activity and potential threats. Organizations should employ Security Information and Event Management (SIEM) tools integrated with cloud-native logging solutions to aggregate logs and detect anomalies in real-time.

- Network Segmentation

Implementing network segmentation in cloud environments helps separate critical systems and workloads into distinct zones, reducing the impact of potential breaches.

- Secure Automated Deployment Practices
- Enforcing secure automated deployment practices through

infrastructure as code is crucial for maintaining a consistent and secure cloud environment.

- Multi-Cloud and Hybrid Cloud Consideration

As organizations increasingly adopt multi-cloud and hybrid cloud environments, it's important to account for the complexities introduced by these setups.

INTERQUEST

Cybersecurity Talent Development

Challenges in Cybersecurity Talent Development

- Skills Gap: The shortage of skilled professionals impacts organizations globally, increasing recruitment costs, staff churn rates, and organizational risks
- Cost of Turnover: Replacing a single cybersecurity employee

can cost between Euro 138K-184K, highlighting the importance of retention.

- Dynamic Threat Landscape: As threats evolve, the demand for adaptable and skilled professionals continues to rise

Effective Strategies for Talent Development

- Upskilling and Cross-Training:

Investing in existing employees through targeted training programs enhances expertise and fosters flexibility Pre-built training plans for roles such as Cybersecurity Foundations, Linux Fundamentals, and CompTIA certifications provide structured learning paths

- Personalized Career Roadmaps:

Tailored development plans aligned with individual career goals improve employee engagement, retention, and satisfaction.

- Hands-On Learning:

Incorporating practical training deepens knowledge retention and accelerates skill development. Examples include cyber ranges and interactive ethical hacking games

- Community-Driven Initiatives:

Collaboration through mentorship programs, open-source projects, and peer networks fosters continuous learning and real-world exposure.

- Retention Strategies:

Offering learning opportunities boosts employee retention rates by up to 66% Building a resilient security culture ensures employees feel valued and supported in their roles.

INTERQUEST

Key Considerations

- **AI Readiness Assessment:**
Evaluate your organization's infrastructure, data management capabilities, and workforce skillsets.

- **Cost-Benefit Analysis:**
Conduct detailed financial analysis to outline the costs of AI deployment against expected benefits.

- **Technology Selection:**
Choose AI tools and technologies that align with your business objectives and ensure scalability and compatibility with existing systems.

- **Training and Upskilling:**
Invest in continuous training programs to update employee skills to match advancing AI technologies.

- **Future-Proofing:**
Establish AI innovation laboratories and technology scouting teams to monitor technological developments and evaluate their potential business impact.

INTERQUEST

Benefits of Artificial Intelligence (AI)

This offers numerous benefits for businesses, revolutionizing operations and driving growth across various sectors.

Here are the key advantages of implementing AI in business:

- Enhanced Efficiency and Productivity
  AI automates repetitive tasks, freeing up employees to focus on more strategic and creative work.
- Improved Decision-Making
  AI analyzes large amounts of data in real-time, providing valuable insights for informed decision-making.
- Cost Reduction
  By optimizing processes and minimizing human error, AI implementation can significantly reduce operating costs.
- Enhanced Customer Experience
  AI-powered tools like chatbots and recommender systems improve customer interactions by providing quick responses and personalized solutions.
- Data Analysis and Insights
  AI processes vast amounts of current and historical data, capturing insights and forecasting future trends or behaviors.

- Personalization and Targeting
  By analyzing consumer data, AI enables businesses to offer more personalized recommendations and targeted messaging to specific customer segments.
- Operational Optimization
  AI touches many aspects of business operations, including supply chain management and workforce scheduling. It can fine-tune inventory levels, route planning, and production schedules, leading to less waste and more efficient resource allocation.
- Increased Profitability
  The combination of improved productivity, reduced costs, higher efficiency, and potential new growth opportunities can lead to increased profitability for businesses leveraging AI effectively.
- New Capabilities and Business Model Expansion
  AI enables organizations to identify new revenue streams and expand their business models by leveraging the vast amounts of data they collect.
- Improved Speed of Business
  AI accelerates business processes, shortening cycles and reducing time from one stage to the next, such as from design to commercialization.

INTERQUEST

Some thoughts……

- ✓ Cybersecurity should enable innovation, not hinder it
- ✓ CISOs must shift from technical advisors to Business enablers
- ✓ Align cyber risk quantification (CRQ) with financial KPIs
- ✓ Did you investigate all the possibilities within your organization

Only 21% of executives align cyber budgets with top organizational risks (PwC)

Making the world a safer place.

If you would like to receive the pdf of this keynote, please link with me on LinkedIn and I will send you the keynote.

Harry Vidler
Managing Consultant InterQuest Group
Harry.Vidler@interquestgroup.com

Dr. Henk Jan Jansen
Founder & CEO
HJ Interim
Dr.Henkjan.jansen@hjinterim.net

INTERQUEST

Discussed Main Topics

1. Introduction Who I am
2. Top Cybersecurity & Innovation Challenges in 2025
3. AI – The Double-Edged Sword
4. What are the AI risks within Business
5. AI-Driven Cybersecurity Solutions & Key Benefits

Break

6. Emerging Technology Trends
7. AI & Cloud Security Strategies
8. Cybersecurity Talent Development
9. Key Considerations
10. Benefits of Artificial Intelligence (AI)
11. Some thoughts……

Dr. Henk Jan Jansen

Founder & CEO HJ Interim

Dr.Henkjan.jansen@hjinterim.net