**Title: Staring at the Clouds: Securing the Bank’s cloud real-estate**

**Abstract:**

When the world’s most storied financial institution decided to embrace the power of the cloud, the security team had to adapt and develop a cloud security framework to ensure their cloud journey was smooth sailing. Join us to hear from the Bank of England on their unique ***3I*** (Inventory, Intelligence Insights) framework to securing their cloud environment.

**Speaker Bio:**

Vincent King, Head of DevSecOps for Cloud Transformation, Bank of England

Vince King is the Head of DevSecOps for Cloud Transformation, Bank of England. Previously a University of Edinburgh graduate in Computer Science and Artificial Intelligence he has more than 20 years’ experience working on software development projects both large and small. As a reformed developer, SDLC advocate, and secure coding trainer, Vince is now Cyber Analyst leading efforts in the use of the Cyber data we gather to support data-driven decision making.

Vince has practical expertise in strategic leadership across multiple cyber security disciplines, including, risk management, cyber resilience, security architecture, Cloud transformation, and vulnerability management across multi-disciplined organisations. He is a CISSP and CITP, and is passionate about mentoring others to achieve recognition for their work through engagement with the British Computer Society.

**Outline:**

1. **Chapter 1: Introduction** 
   1. Introduction to the Bank of England
   2. Speaker Introduction
   3. Overview of the Bank’s Journey to the cloud
2. **Chapter 2: What keeps the security team awake at the Bank**
   1. Threats: What are the cloud threats that need to be considered
      1. Misconfigurations
         1. The risk with misconfigurations with easy to deploy security
      2. Lack of Visibility
         1. Where does traditional network security tools fall apart
      3. Malicious insiders
3. **Chapter 3: The 3Is of Monitoring in the cloud** 
   1. Inventory
      1. Why agent-based solutions are not sufficient for modern cloud applications
      2. Multi-cloud: The need to manage inventory across a multi-cloud environment
   2. Intelligence
      1. Staying ahead of new vulnerabilities
      2. Detect vulnerabilities in the existing code base

Due to the pace of change, any business that has developed software for more than 12 months will have legacy code. As an institute that is more than 325 years old, we have our fair share. Moving applications to the cloud is the perfect opportunity to re-develop and re-engineer your applications, but for those that have to be “lifted-and-shifted”, we need to ensure that there are no new, or existing vulnerabilities. For software of any level of complexity, a manual process will prove too cumbersome. Automation is the key, and can be started easily and cheaply by using SAST (Static Application Security Testing) tools as part of your build pipeline.

* + 1. Time to exploit has reduced significantly
  1. Insight
     1. The power of context
     2. Prioritize which resource to secure first.
     3. Visualizing attack paths

1. **Chapter 4: The Banks’ requirements for a modern cloud security platform** 
   1. Connectivity to the entire cloud real estate across cloud providers
      1. Visibility into every cloud resource and storage / database

Cloud brings lots of benefits, but also the potential for getting things wrong. The ephemeral nature of cloud resources means that VMs, databases, AI bots, fileshares can all be spun up in seconds. This provides a security challenge. Knowing what you have, and if it is vulnerable is essential.

* + 1. Visibility into modern cloud native workloads
    2. Visibility into AI services
  1. Identify resources, (Active and Stale) along with the configuration, ownership and complete context
     1. Why does context matter
  2. Insights: Overlay context gathered with threat intel and identify key attack paths. Identification of:
     1. Misconfigurations
     2. Exposed attack
     3. Vulnerabilities
     4. Risk/Issues in the software pipeline

1. **Chapter 5: The selection of Wiz to be the cloud security platform** 
   1. Why Wiz
2. **Chapter 6: Looking ahead, what is the next journey for the Bank’s cloud security approach**
   1. Workloads
   2. Attack surface to secure
   3. Shift left
   4. Detection and response
   5. Integrations