Operational Security & Compliance for AcmeBank's Tokenized Bonds

Powered by OpenZeppelin's Open-Source Monitoring & Automation Stack

Presented by

Zachary Wolff

The Challenge: Entering Digital Assets

Regulatory Uncertainty - Existing financial regulations weren't designed for blockchain technology

Market Pressure - Competitors are already tokenizing assets while you evaluate options

New Attack Vectors - Smart contract vulnerabilities and on-chain risks don't exist in traditional finance

Operational Complexity - Need 24/7 monitoring of immutable transactions with instant response capabilities

No Established Playbook - Traditional security vendors don't understand blockchain-specific threats

OpenZeppelin Meets These Needs

- Built-in compliance monitoring for regulatory requirements

- Production-ready tools used by major financial institutions

- 10+ years securing $100B+ in on-chain value
- Automated 24/7 monitoring with millisecond response times

- Open-source transparency with enterprise support available

Learn more

LIve Demo of Tokenized Bond Contract

Critical Compliance & Security Scenarios 1

1

Missed Interest Payments
Detect overdue payments, alert operations team

2

Large Unauthorized Transfers
Transfers >$10M trigger emergency pause

3

Regulatory Threshold Breaches
Entity ownership >20% blocks further purchases

LIve Demo of Tokenized Bond Contract

Critical Compliance & Security Scenarios 2

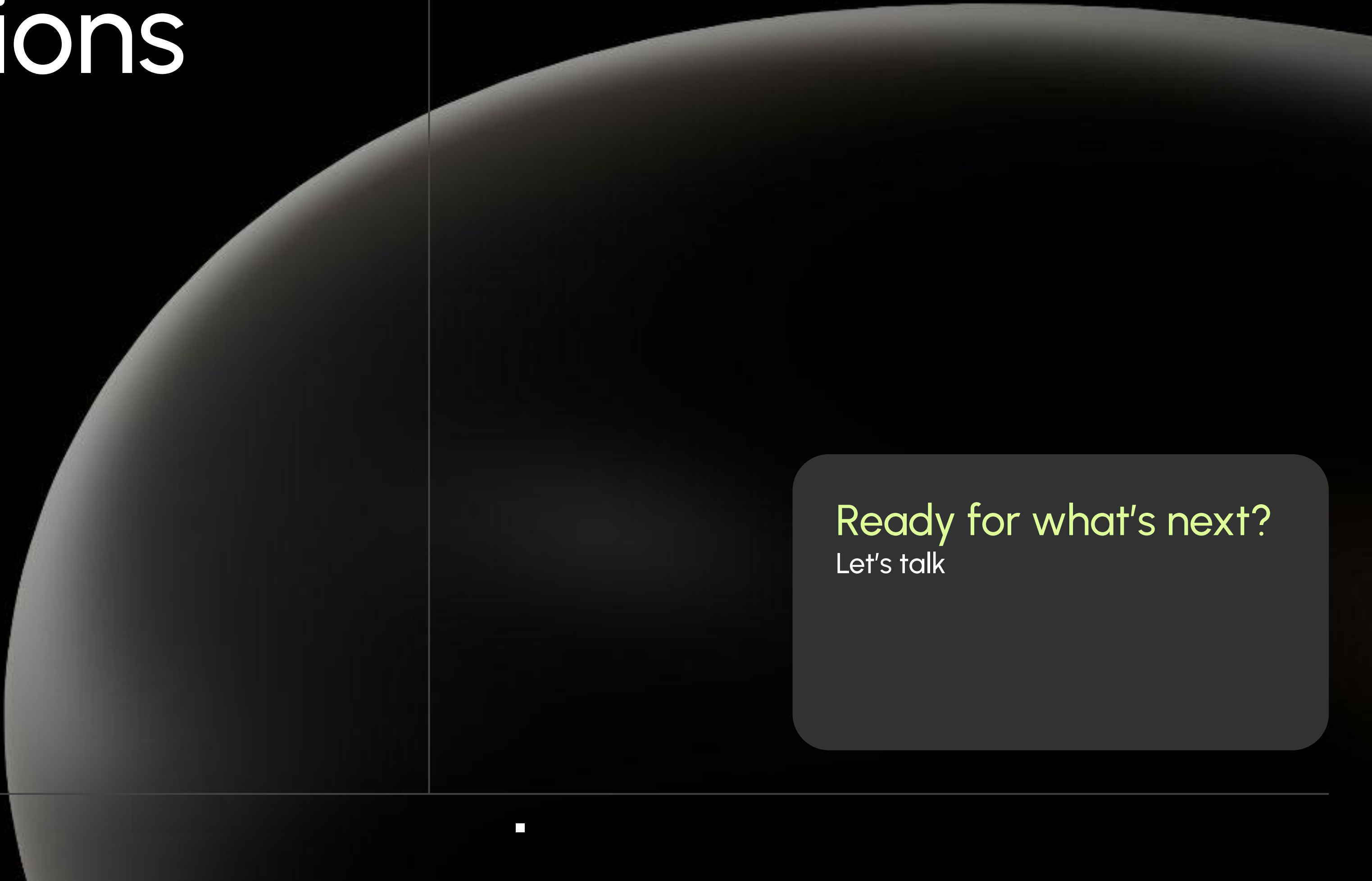
4

Private Key Compromise
Detect actions outside change control windows, emergency response

5

OFAC Sanctions Screening
Block interest payments to sanctioned addresses automatically

Questions



Ready for what's next?

Let's talk