Sean Andrews

Manager
7039700443
sean.andrews@us.forvismazars.com

Sean is a leader in offensive security and cybersecurity, with over seven years of hands-on experience across diverse industries including finance, healthcare, and commercial sectors. As manager of IT Risk & Compliance at Forvis Mazars, Sean specializes in advanced penetration testing, web application security, and smart contract security, consistently delivering unmatched value and protection for clients.

He is an Artificial Intelligence Subject Matter Expert, frequently leading engagements that integrate AI into enterprise risk strategy and operations. He has pioneered client service offerings in AI governance, deepfake creation and detection, cloud penetration testing, agentic automation, and other emerging cybersecurity domains. Sean's expertise extends to developing and implementing AI risk management frameworks, steering committee augmentation, and strategic use case identification for enterprise clients.

As a skilled public speaker, Sean regularly presents on cybersecurity, offensive security, and AI topics at industry conferences and client events. His ability to translate complex technical concepts into actionable insights empowers organizations to navigate evolving threats and regulatory landscapes with confidence.

His unwavering commitment to client experience is evident in every engagement. He is dedicated to building trusted partnerships, delivering tailored solutions, and ensuring clients receive the highest standard of service and support.

Career Highlights

- Led and executed advanced penetration testing engagements across web applications, APIs, internal and cloud networks, and physical environments, leveraging offensive security methodologies to identify and remediate vulnerabilities for clients in finance, healthcare, and commercial sectors.
- Developed and delivered AI governance assessments for clients, providing both strategic long-term guidance and tactical support—including policy development, regulatory artifact creation, and frameworks for risk-based decision making in AI implementations.
- Designed and implemented deepfake creation and detection services, and conducted comprehensive social engineering campaigns via email, physical, and AI-driven (deepfake) vectors to assess and strengthen client resilience against emerging threats.
- Authored the firm's playbooks for cloud penetration testing and web application testing, establishing best practices and methodologies for evaluating the security posture of Azure, AWS, and externally facing client applications.
- Participated in a blockchain fellowship, helping to develop the firm's capabilities in smart contract review and blockchain security. Enabled clients to understand smart contract mechanics, assess blockchain's impact on security controls, and stay ahead of evolving regulatory trends.

- Regularly provides public speaking and training on offensive security, AI governance, deepfake risks, and blockchain security, empowering clients and industry peers to navigate complex cybersecurity challenges.