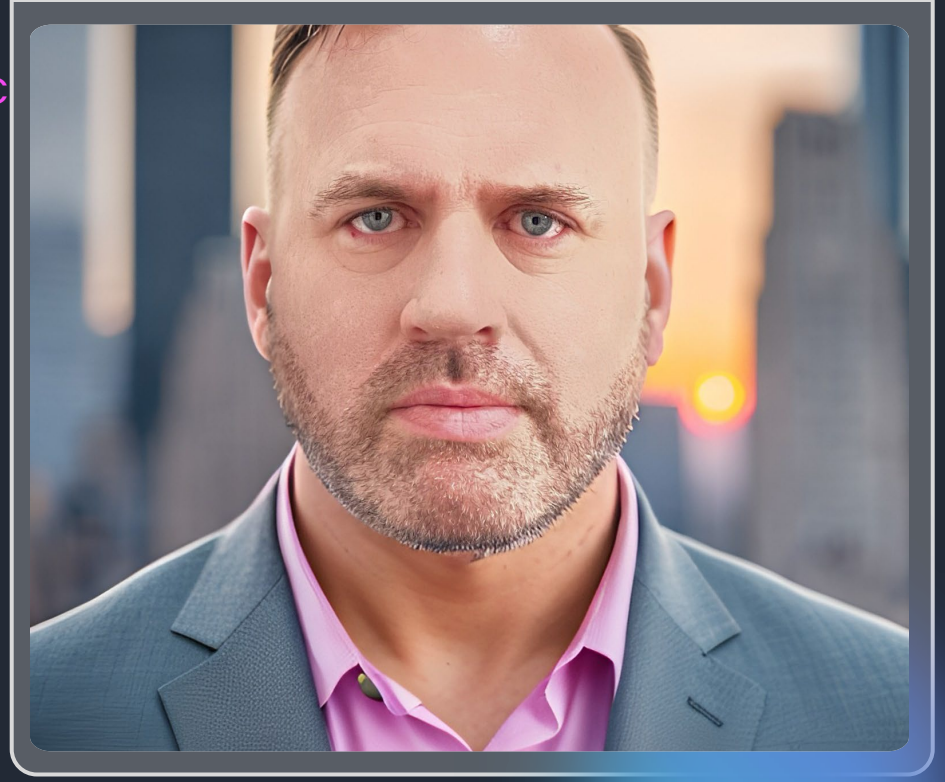
NEW YORK METRO JOINT CYBER SECURITY CONFERENCE

Cyber Incident Masterclass: Real-World Response Tactics from Industry Leaders

September 26, 2024 , at 1:30pm

INFOSECURITY.NYC

ASYMMETRIC RESPONSE



THOMAS RYAN

MODERATOR

https://www.linkedin.com/in/tommyryan/

Thomas Ryan, CEO and Founder of Asymmetric Response, is a leader in offensive cybersecurity with over 25 years of experience. A third-generation Navy veteran, he is known for his strategic approach and his pioneering Robin Sage Experiment, which exposed social media vulnerabilities. His published CVEs and references in the MITRE ATT&CK framework highlight his significant impact. At Asymmetric Response, Ryan fosters innovation and mission success, delivering cutting-edge solutions across industries. A sought-after speaker and thought leader, he focuses on AI risk, security, and hybrid IT/OT environments, shaping the future of cybersecurity.

ASYMMETRIC RESPONSE

VLAD BRODSKY

PANELIST

https://www.linkedin.com/in/vlad-brodsky/

Vlad Brodsky is the SVP, Chief Information Officer and Chief Information Security Officer at OTC Markets Group, a regulated publicly traded financial institution that operates the world's largest OTC equity electronic marketplace. His responsibilities include leading the firm's information security strategy, program, and processes as well as running the firm's IT operations and infrastructure. Vlad has expertise in Information Security, Risk Management, IT Infrastructure Management and Financial Services. Prior to OTC Markets Group, he worked as a Chief Security Officer at Innovest Systems, a SaaS provider in the Trust Accounting and Wealth Management space.

ASYMMETRIC RESPONSE

MICHELLE SCHAAP

PANELIST

https://www.linkedin.com/in/michelleschaap/

Ms. Schaap is a seasoned attorney with over 30 years of experience specializing in privacy and data protection, cybersecurity preparedness, and incident response. As a breach coach, she advises clients on asset inventory, risk assessments, policy drafting, personnel training, and cyber insurance, helping businesses prepare for and respond to breaches. Her practice spans various sectors, including construction law, where she drafts and negotiates agreements for complex projects, and renewable energy, with expertise in power purchase and EPC agreements. Additionally, she handles software licensing and technology agreements, commercial transactions, franchising, and employment law. A frequent speaker on cybersecurity and data protection, she is recognized for her in-depth knowledge across these fields.

ASYMMETRIC RESPONSE

ALEX WAINTRAUB

PANELIST

https://www.linkedin.com/in/alexwaintraub/

Alex Waintraub is a cybersecurity professional with over a decade of experience in IT, Security Operations, and DFIR. He specializes in managing security teams, enhancing SOCs, developing Incident Response Plans, and refining threat intelligence operations. With 8 years of leadership experience, he has honed cyber threat hunting and escalated incident response methods across industries. Alex combines technical expertise with strategic acumen, delivering cybersecurity services to global enterprises. He is a frequent conference speaker and hosts the NJ Cyber Fireside Chat. He holds a bachelor's degree in Information Technology and Network Security from New York Institute of Technology.

ASYMMETRIC
RESPONSE

We often hear that leadership, preparation, and execution are crucial in a crisis. From your experience, what makes the biggest difference when an incident hits, and how should organizations prepare for the unexpected?

ASYMMETRIC
RESPONSE

Incident Response Strategy and Leadership

Vlad, you hold the dual roles of both CIO and CISO. How do you balance operational IT needs with security, especially when responding to a cyber incident in a financial services organization? What challenges have you faced, and how did you overcome them?

Incident Response Strategy and Leadership

Michelle, from a legal standpoint, how important is the role of a legal counsel in incident response, and how do you ensure that legal strategies align with quick decision-making during an incident? Can you share a scenario where legal and business objectives were in conflict, and how was that resolved?

ASYMMETRIC
RESPONSE

Operational Tactics in Incident Response

Alex, you have deep experience running SOCs and building incident response plans. What are the top priorities when a security team first identifies a cyber incident? How do you ensure proper escalation and containment without causing further business disruption?

Operational Tactics in Incident Response

Vlad, once an incident is contained, how do you guide the recovery phase while maintaining business continuity? What are some strategies for balancing system restoration with ensuring the root cause of the incident is fully addressed?

ASYMMETRIC
RESPONSE

Legal and Compliance Challenges

Michelle, you work with a range of clients on compliance and cyber incident recovery. What are some of the most common mistakes organizations make post-incident, particularly concerning regulatory compliance, and how can they avoid these pitfalls?

Legal and Compliance Challenges

Alex and Michelle, vendor risk is often a significant challenge during an incident. How do you both advise companies to handle third-party vendors during an attack and what are some of the key legal and operational considerations in those situations?

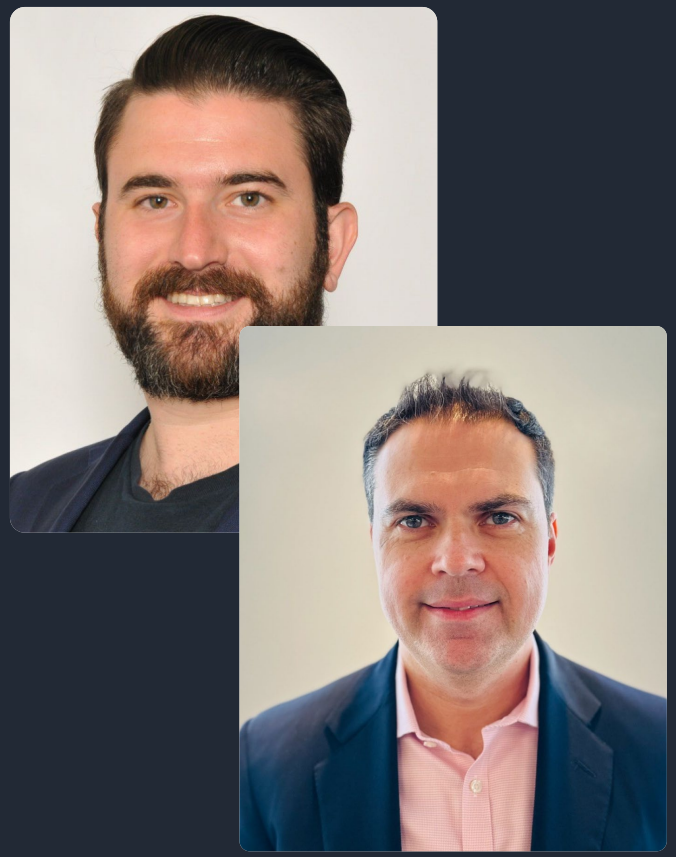
ASYMMETRIC
RESPONSE

Proactive Defense: Preparation & Threat Hunting

You've built threat-hunting teams and run security operations. How important is proactive defense, and what should organizations focus on in terms of threat hunting to stay ahead of evolving threats?

ASYMMETRIC
RESPONSE

Proactive Defense: Preparation & Threat Hunting



Vlad, Alex, many organizations struggle to get their leadership teams to invest in red teaming and proactive defense measures. How do you both advocate for building these into an organization's budget and strategy, especially when ROI is not immediately clear?

Wrap-Up and Key Takeaways

If you could give one piece of advice to CISOs or security leaders preparing for their next major incident, what would it be?

ASYMMETRIC
RESPONSE

Thank You!

Any Questions?