



Overview

Format: Executive Briefing or Keynote

Duration: 45–60 minutes (adaptable to 30 minutes)

Audience: Boards, executives, senior leaders, legal and risk stakeholders

Executives are often asked to make high-stakes decisions during cyber incidents without a clear understanding of what evidence can reliably support those decisions.

Digital Forensics for Executives demystifies how modern investigations actually work, what “confidence” means in DFIR, and why timelines, scope, and conclusions evolve as incidents unfold. Drawing on real investigations, this session explains the limits of forensic certainty and how leaders can better interpret technical findings under pressure.

The focus is not on technical depth, but on decision-quality: helping leaders ask better questions, set realistic expectations, and support defensible outcomes.

What This Session Covers

Participants gain a practical understanding of how evidence is collected, analysed, and interpreted during incidents, including why early conclusions are often wrong and how investigative confidence increases over time. The session also explores common misunderstandings between executives, responders, legal teams, and external advisors that slow response and increase risk.

Rather than treating forensics as a black box, the talk frames it as a decision-support capability that leaders must actively enable.

Key Takeaways

Attendees leave with a clearer understanding of what digital forensics can and cannot provide, how to interpret investigative findings responsibly, and how executive behaviour influences investigation quality, speed, and defensibility.

Why This Talk Resonates

This session resonates because it bridges a persistent gap between technical teams and leadership. It equips executives with the context needed to make informed decisions without requiring technical expertise, reducing friction and improving trust during real incidents.

Delivery Style & Customisation

Clear, calm, and non-technical. Content can be tailored for boards, executive teams, legal audiences, or regulators, and adapted to enterprise or critical-infrastructure contexts.

Presented by Seth Enoka

Director & Principal Analyst, Lykos Defence

Author, Cybersecurity for Small Networks (No Starch Press)