

# What's Really Happening in OT Cyberattacks

Lessons from the Field, Not the Headlines



## Overview

**Format:** Keynote or Conference Session

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

**Audience:** Security leaders, OT/ICS practitioners, executives responsible for critical infrastructure

Cyberattacks against OT are frequently described in dramatic terms, but the reality on the ground is more nuanced, and more actionable.

**What's Really Happening in OT Cyberattacks** cuts through hype and speculation to examine how adversaries actually gain access to industrial environments, what they do once inside, and where defenders consistently struggle. Drawing on real investigations, readiness work, and incident response in critical infrastructure environments, this session focuses on patterns that matter rather than edge-case scenarios.

The goal is not fear, but clarity: helping organisations understand real attacker behaviour and make better defensive decisions.

## What This Session Covers

Participants are walked through common attack paths into OT environments, including initial access, lateral movement, and operational impact. The session highlights where IT-centric assumptions break down, how visibility gaps and organisational boundaries slow response, and why many industrial incidents escalate unnecessarily.

Rather than focusing on exotic malware, the talk emphasises how routine weaknesses, poor preparation, and mismatched response models create risk in OT environments.

## Key Takeaways

Attendees leave with a clearer picture of current OT threat activity, the most common failure points observed in real incidents, and practical steps to strengthen preparedness and response without disrupting operations. The focus is on achievable improvements that materially reduce risk.

## Why This Talk Resonates

This session resonates because it replaces sensationalism with experience. It speaks directly to both technical and non-technical stakeholders, aligning security teams, engineers, and leadership around a shared understanding of risk and response in industrial environments.

## Delivery Style & Customisation

Clear, practical, and grounded in real cases. Content can be tailored for specific sectors such as energy, transport, manufacturing, or water, and adapted for executive, practitioner, or mixed audiences.

**Presented by Seth Enoka**

Director & Principal Analyst, Lykos Defence

Author, Cybersecurity for Small Networks (No Starch Press)