Successful Strategies in Enterprise Intrusion Investigations

SANS WhatWorks in Forensics and Incident Response Summit 2008

Michael Cloppert
Member Technical Staff
Lockheed Martin Computer Incident Response Team
Phase 2: Establish a presence

- Compromise Systems
- Establish a Presence
- Steal data
But how?
So what now?

We have a process!

Oh you mean this one?

Yeah, it’s broken.
Get Intelligent

Integration of intelligence acquired through analysis and collaboration is key to successfully managing incidents.