







1. Preserving the Knowledge of Exiting Employees

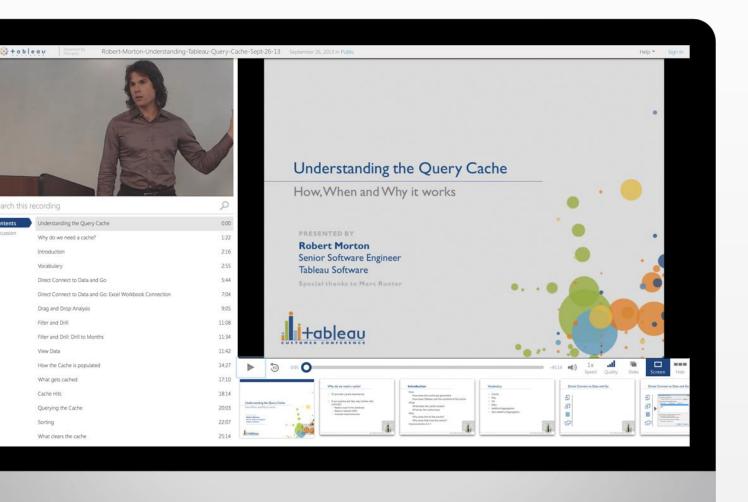
40 hours of offboarding video

125 wpm x 60 minutes x 40 hours = 300,000 words

The equivalent of a 1,200 page document...

...but with 40 hours of moving pictures

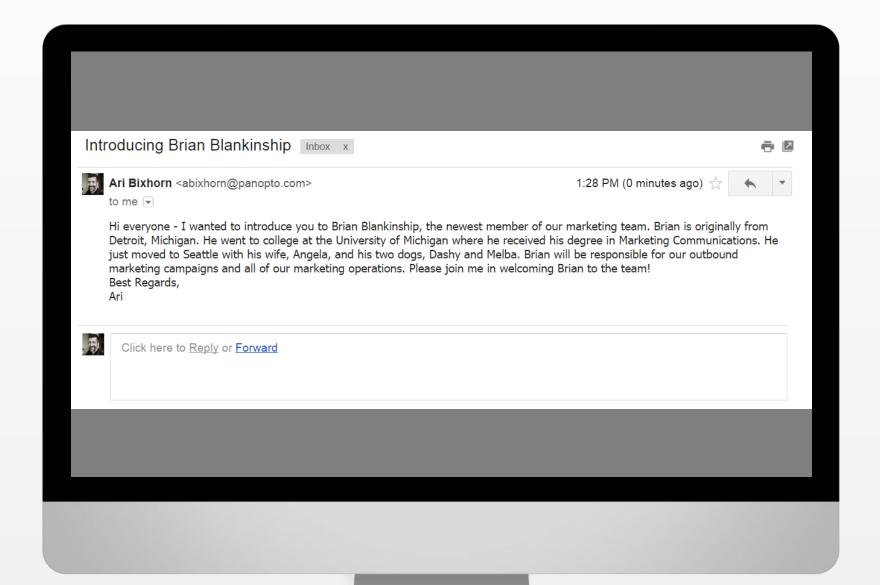




Tripled employees in one year

Target: 30-day ramp-up

Complex analytics product



http://panop.to/brian-intro





Each records a 5-10 minute learning video

Result: 1,000 mini-learning modules

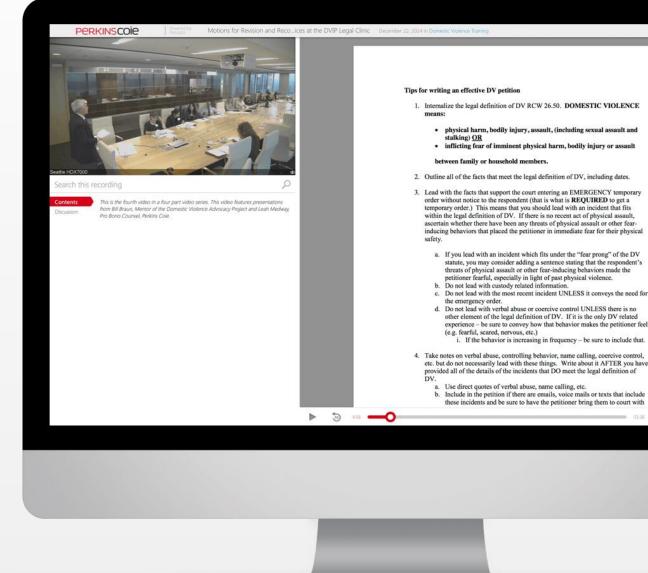
Near zero incremental cost

Expanding beyond formal learning

Meeting recording for attendees

Informal HR benefits videos

Attorney-to-attorney social learning





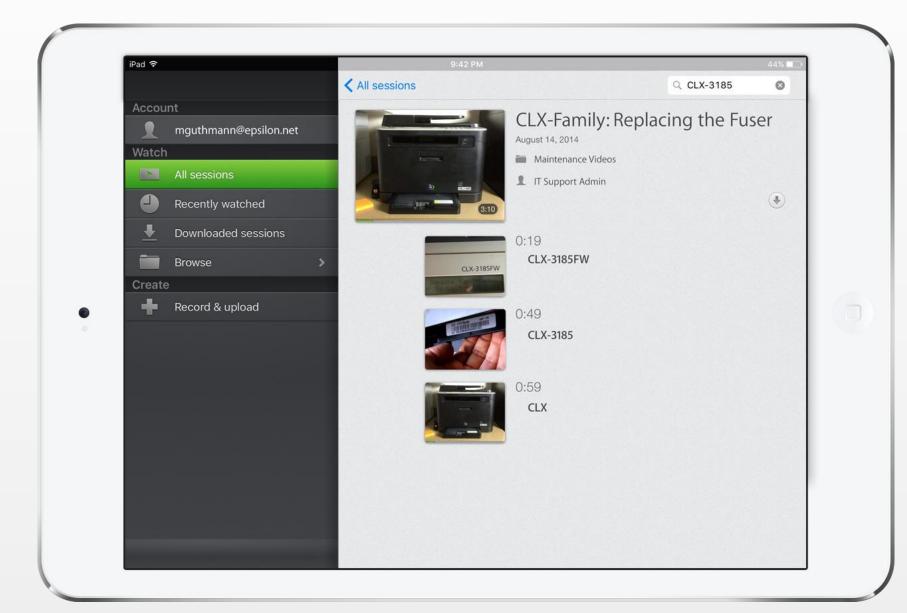
4. Mobile Learning



Mobile printer technicians

Range of models, issues

Carrying stacks of manuals

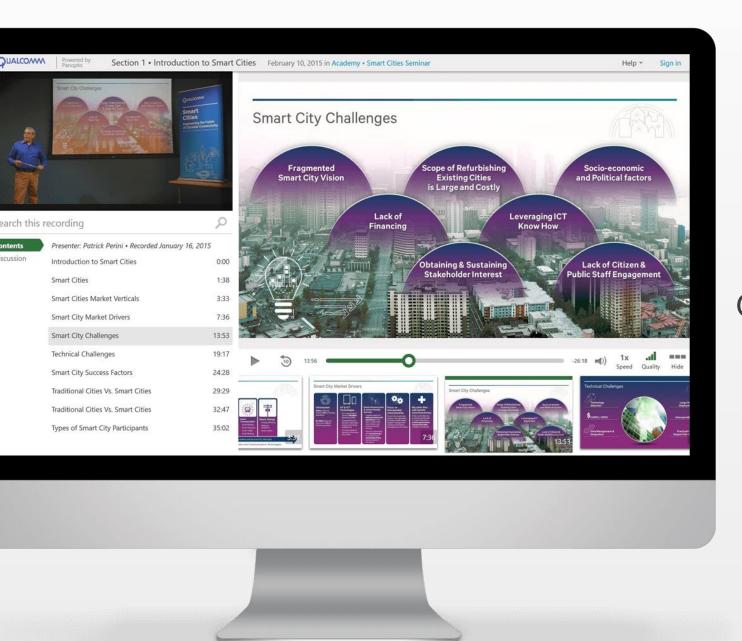








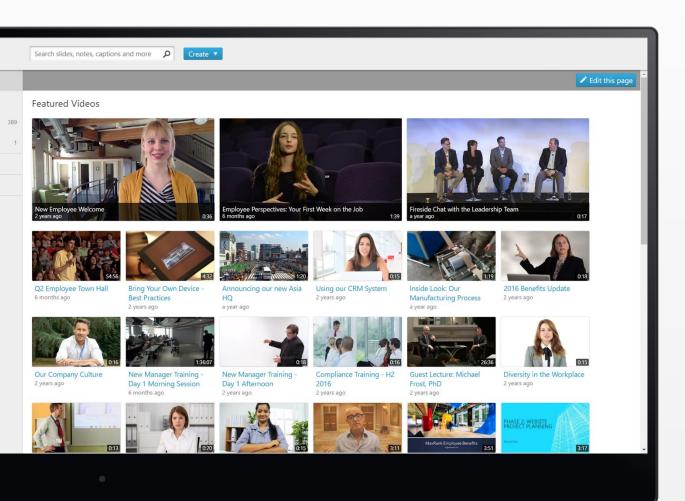




Qualcomm Wireless Academy

5 Enabling Trends





The Rise of the Corporate YouTube



Network —Security

This chapter presents a broad description of network security in the context of today's rapidly changing network environments. he security paradigm is changing, and security solutions today are solution driven and designed to meet the requirements of business. To help you face the complexities of managing a modern network, this chapter discusses the core principles of security—the CIA triad: confidentiality, integrity, and availability.

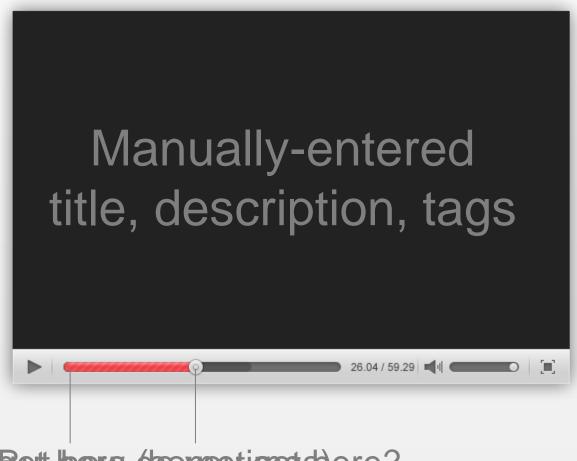
Chapter - 26

Intrusion Detection



An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. NIDS is a network security system focusing on the attacks that come from the inside of the network (authorized users). Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring

system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, sedocumenting existing threats and a necepring individuals from violation reganization. Policies. IDPSes her



Helps you Bett here (soynoetigeets) ere?













Handbook

Comments and Questions

You can also reach me anytime at abixhorn@panopto.com www.panopto.com