SANS 360: ICS Forensics

Robert M. Lee

RobertMichael.Lee@gmail.com
@RobertMLee

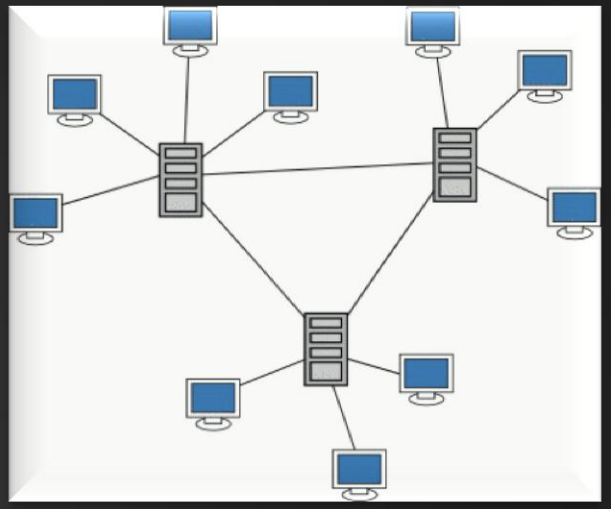
The challenge posed to me…

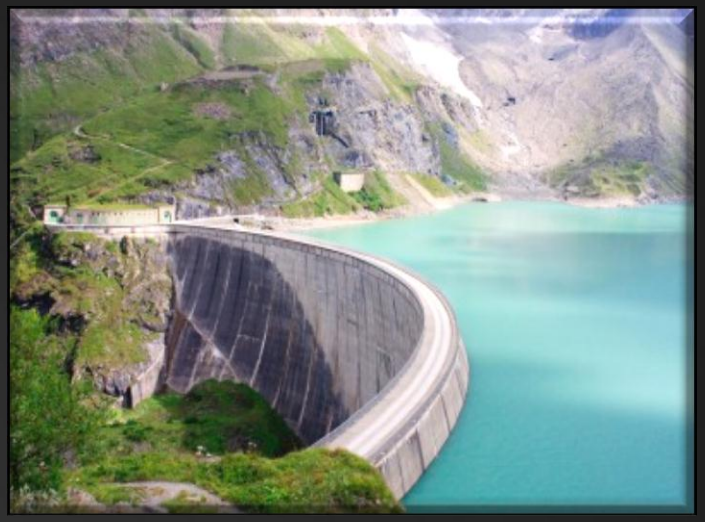
“Rob, go do defense for critical infrastructure”

Do what?

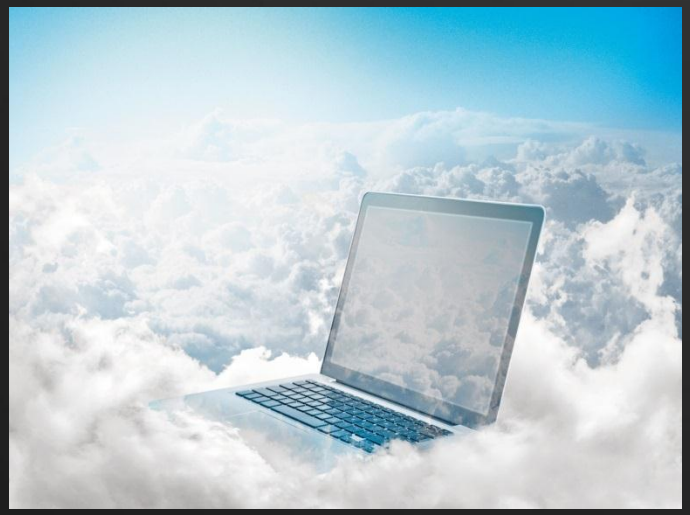
“ICS and SCADA networks…go”

What is ICS?



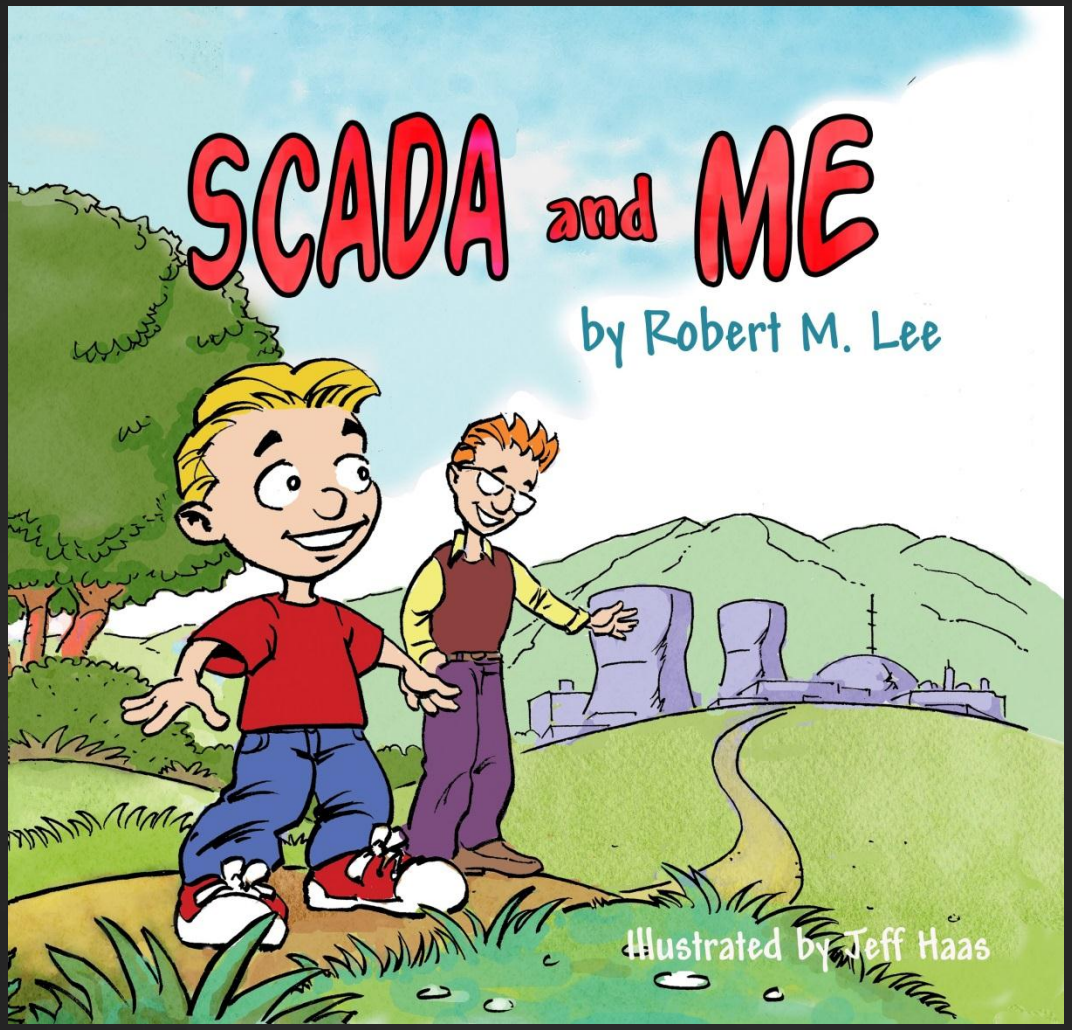


What about SCADA?

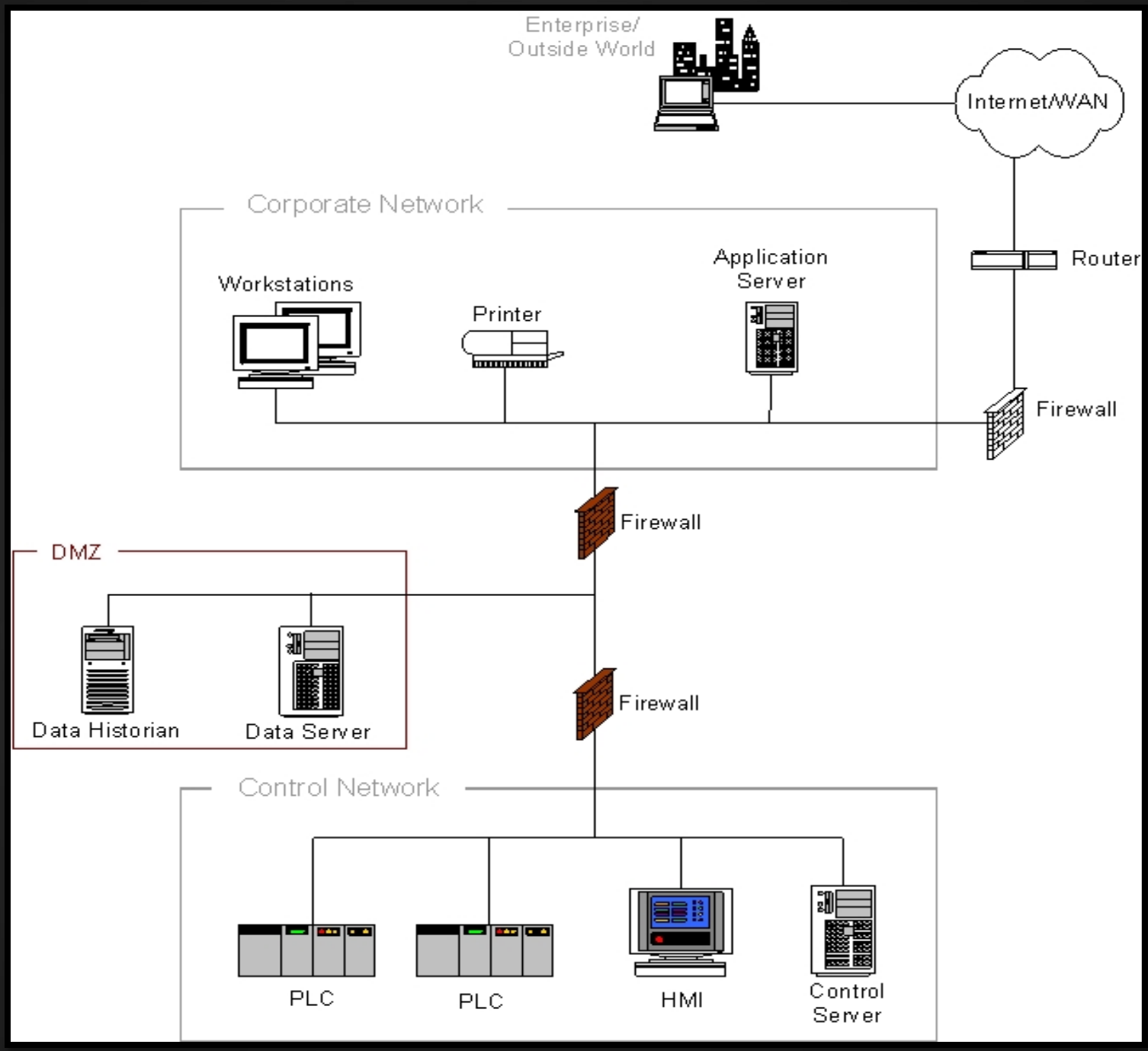


If your answer is the third picture or

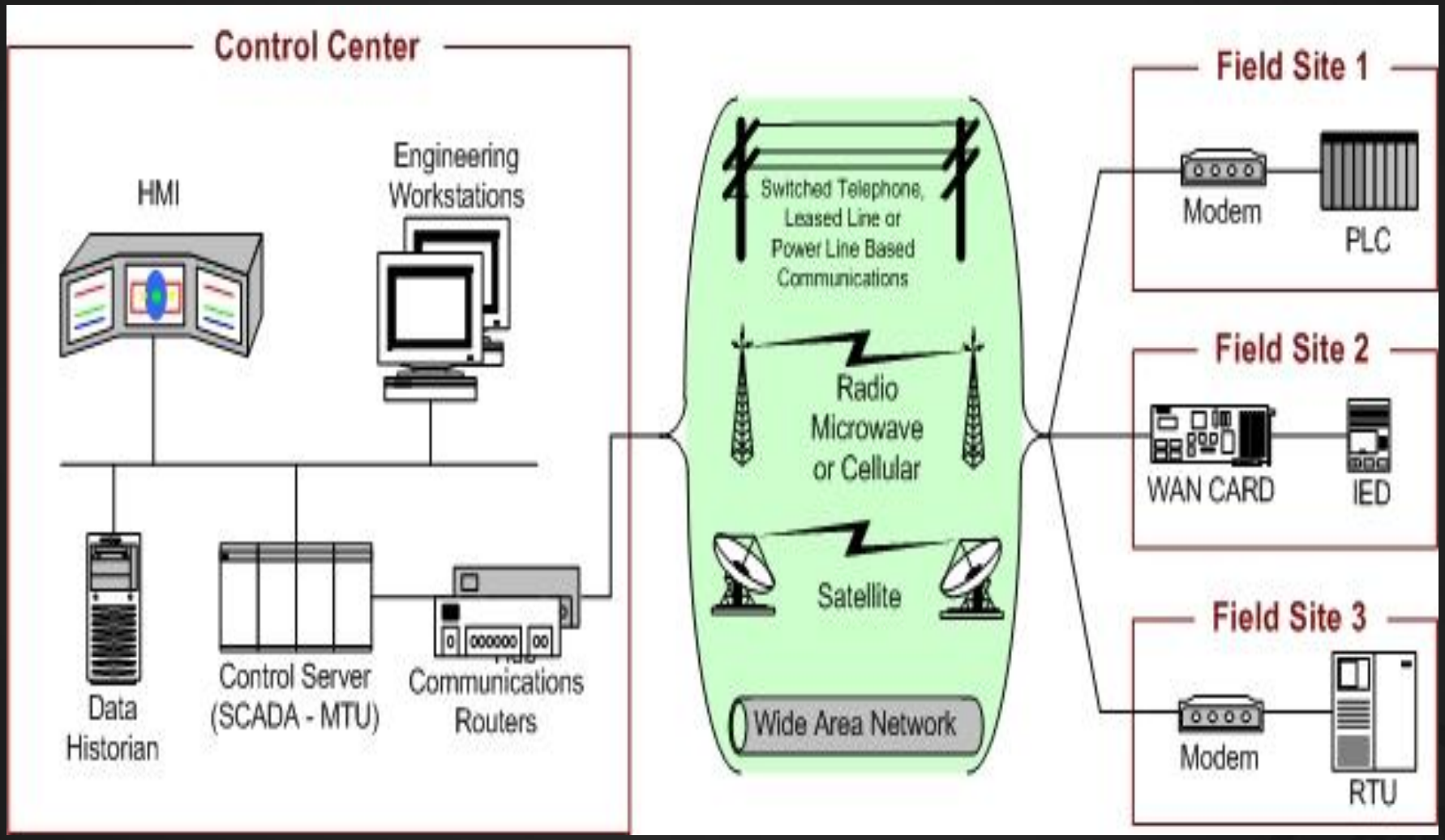
If you still don’t understand…


SCADA and ME
by Robert M. Lee
Illustrated by Jeff Haas

A bit more complex…


Enterprise/
Outside World
Internet/WAN
Corporate Network
Workstations
Printer
Application
Server
Router
Firewall
Firewall
DMZ
Data Historian
Data Server
Firewall
Control Network
PLC
PLC
HMI
Control
Server

Source: NIST

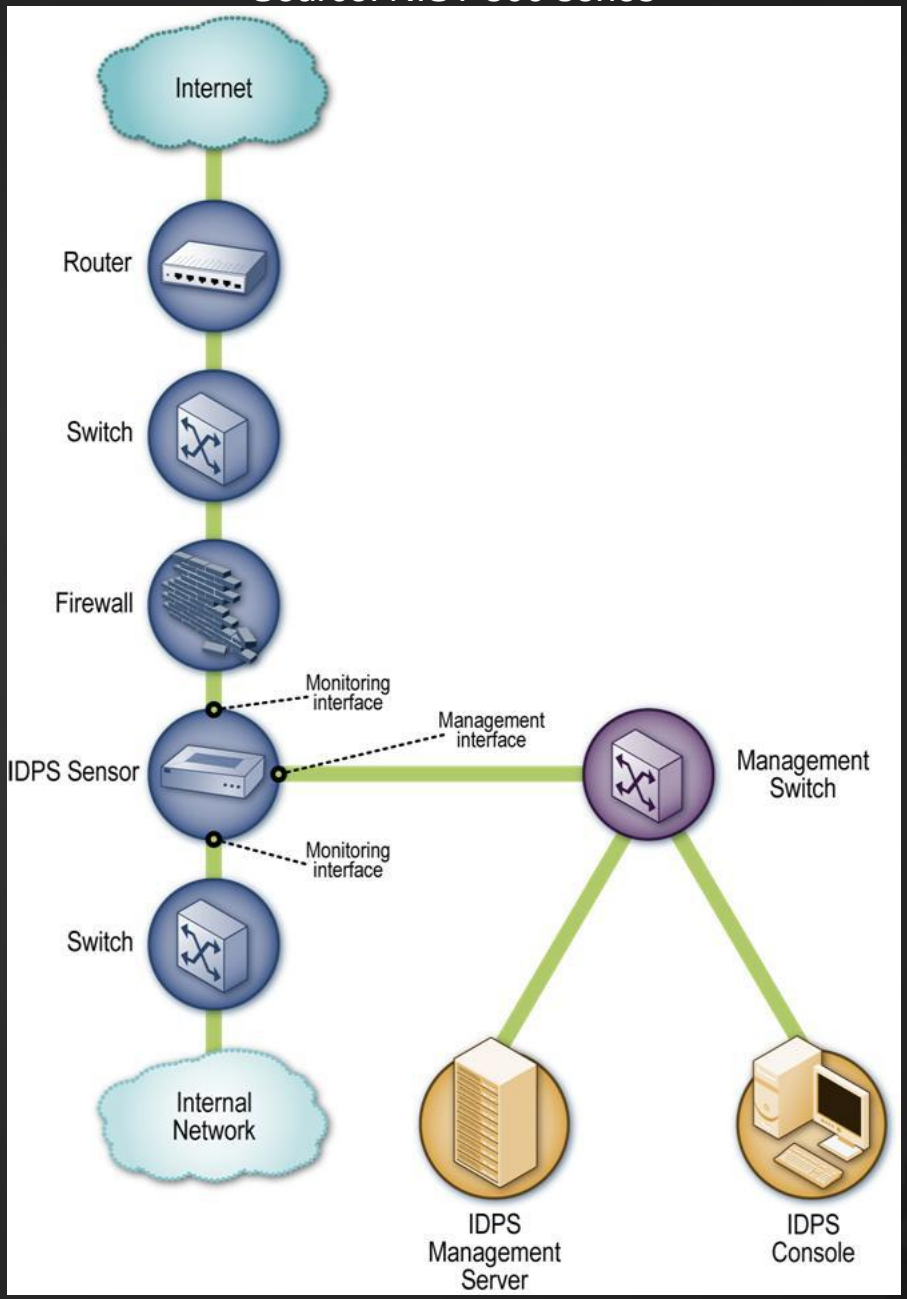

Control Center
HMI
Engineering Workstations
Data Historian
Control Server (SCADA - MTU)
Communications Routers
Switched Telephone, Leased Line or Power Line Based Communications
Radio Microwave or Cellular
Satellite
Wide Area Network
Field Site 1
Modem
PLC
Field Site 2
WAN CARD
IED
Field Site 3
Modem
RTU

Source: NIST

What did you see? How do you defend?

Source: NIST 800 series

Defense or Forensic Device?



Forensics = Defense

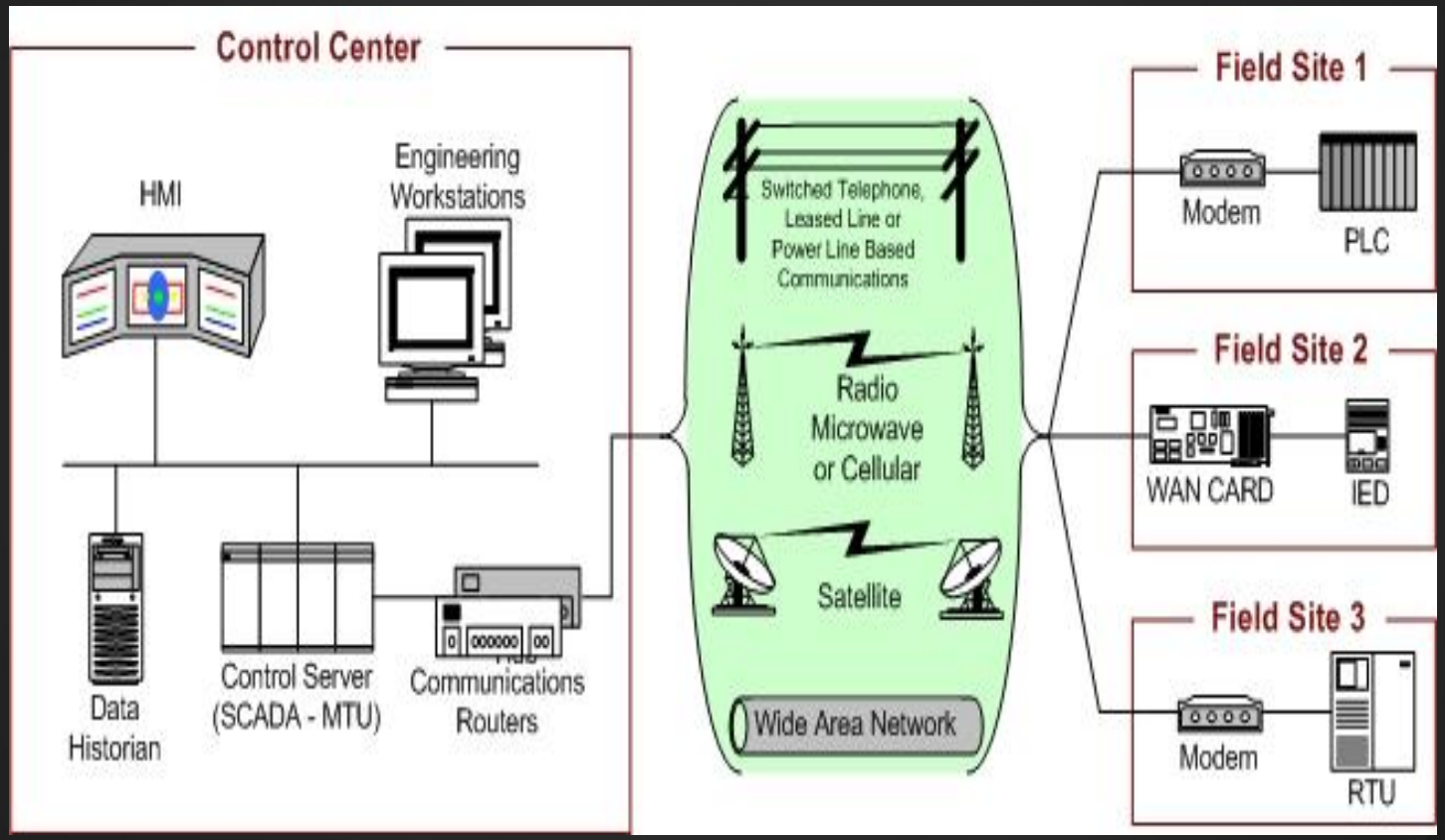
Find the adversary to develop defenses; network defense sensors contain intel

Watching exfil (*cough FOR 508*) is a good starting place for incident response and defense

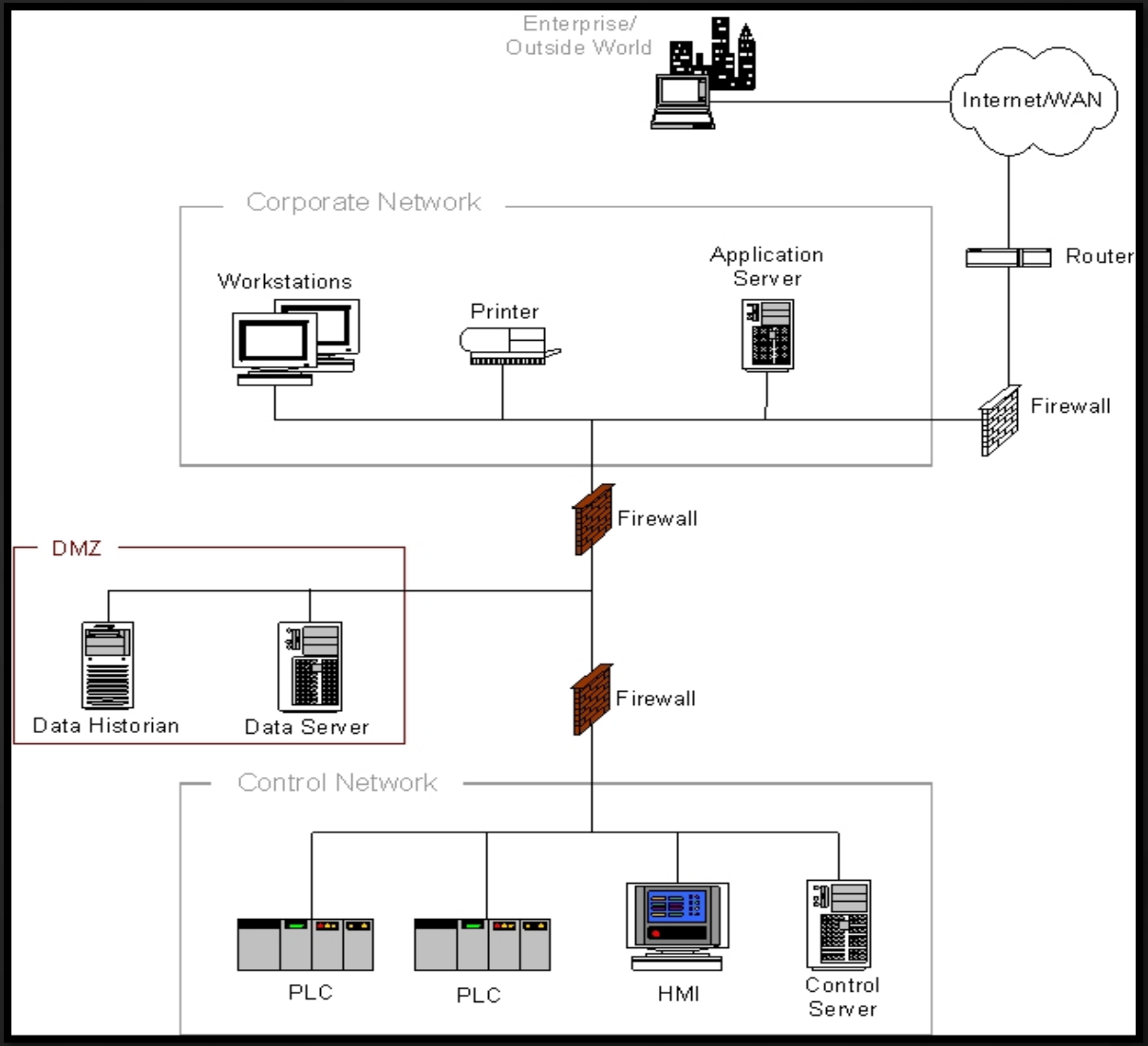
Turn your sensors into forensic devices

Sensors with rules of what you expect or do not expect to see

If your adversary is here…



Identify them, catch them, beat them back here…



Summary

Digital Forensics is key to defense!

ICS Networks are unique but discovering threats is network neutral

You MUST have forensic devices…evidence collection points…ability to test theories

Questions?