Attacking the ICS, a Demonstration

2nd August 2018

ECL
ENGINEERING CONTROL

Introduction

- **Gavin Dilworth – ICS Cyber Security Engineer**
  - Senior Control System Engineer (Rockwell, Wonderware)
  - Originally Studied I.T. – Windows NT/2k, RedHat 7.2, Networking, VPN's and Firewall's
  - O.E. (UK): Shifted towards Cyber Security

- **Industry Certifications**

ECL ENGINEERING CONTROL

Agenda

- **Patching & Anti-Virus/Anti-Malware**
- **Demo –** (Patching & Anti-Malware)
- **Network Segmentation**
- **Demo –** (ICS Attacking)
- **Mitigations**
- **Advanced / Active Defence**
- **Questions**

ECL
ENGINEERING CONTROL

Anti-Virus / Anti- Malware

- Vendor Approved Anti-Virus
- Windows Defender when you don't have the budget
- Use a Sheep-Dip PC for file transfer where you have to (different AV)

- Lowers risk of malicious code execution, based on signatures
- Modern AV now use AI and heuristics

Fundamentally like PPE, shouldn't be relied upon to protect you, last line of defence

ECL ENGINEERING CONTROL

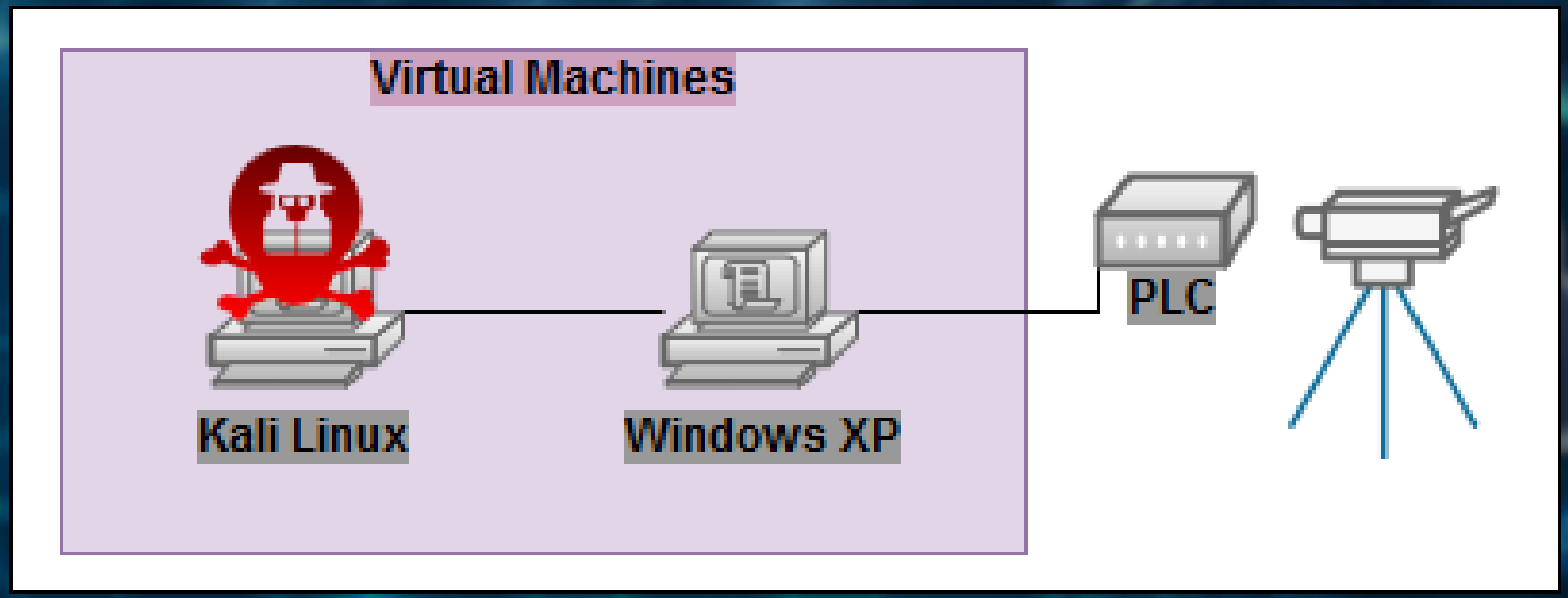
Patching

- Planned Patching is Good.
- Rushed Patching is Ugly
- Vendor approved patching recommended
- Use Staggered Patching to lower risk for unknowns

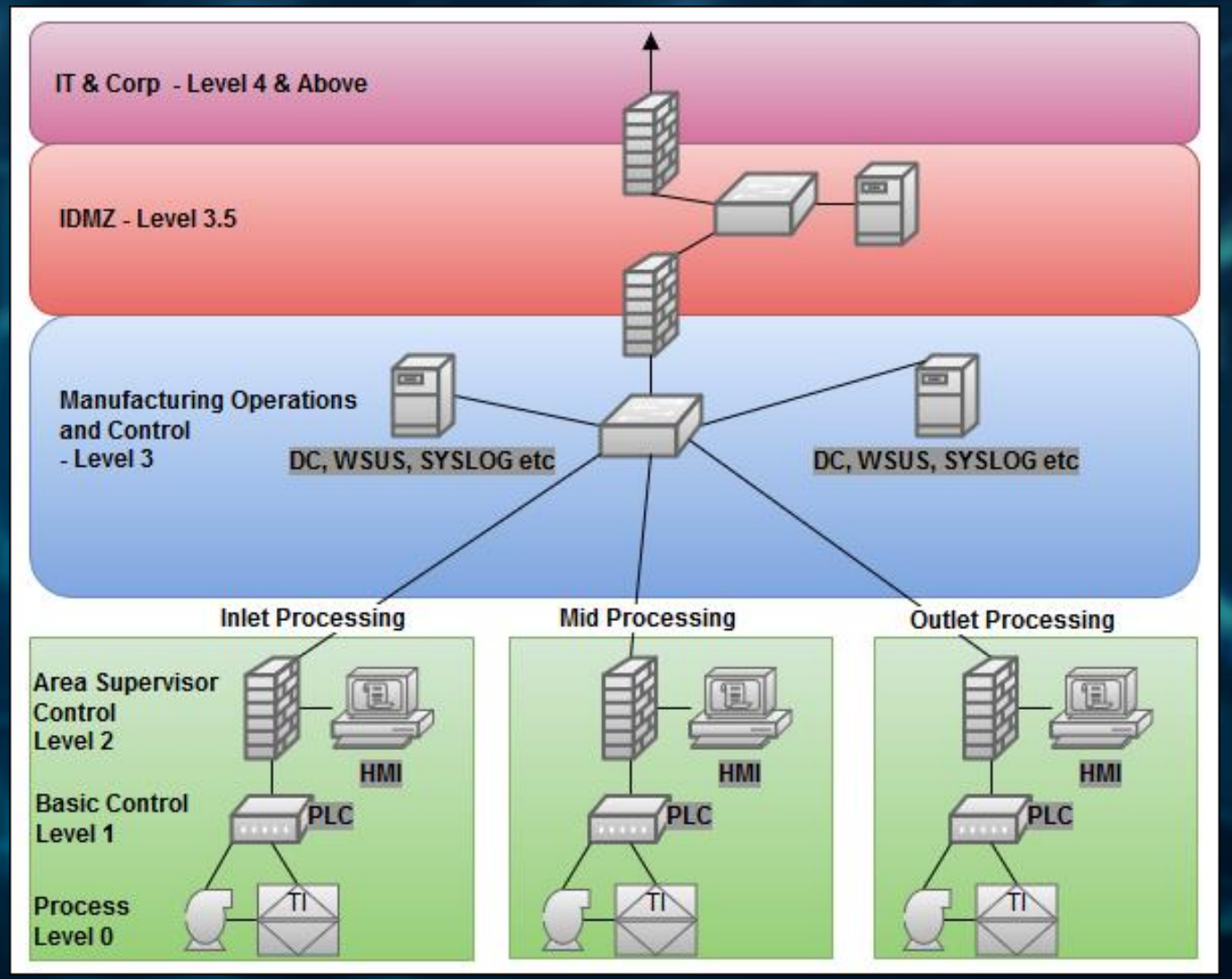
Decreases the risk of automated attacks (Ransomware, human error and script kiddies)

ECL ENGINEERING CONTROL

Demo – Patching & Anti-Malware



Network Segmentation - Purdue Model



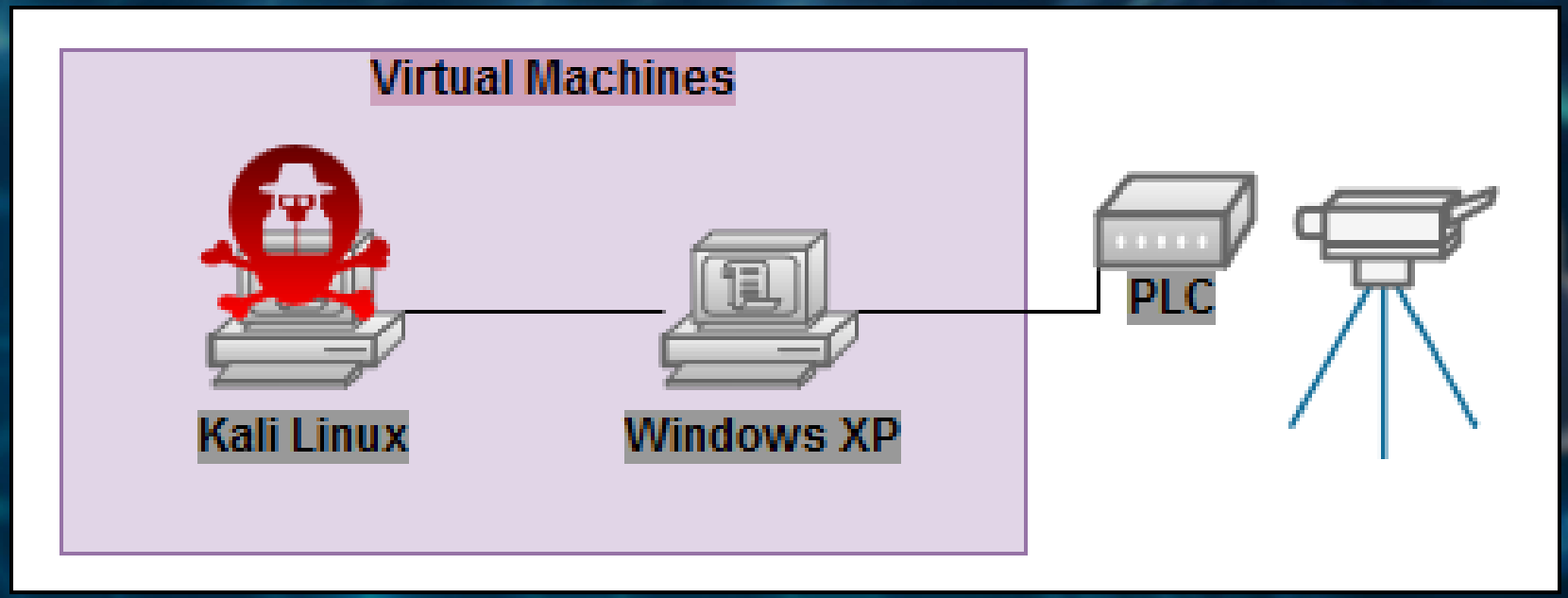
ECL ENGINEERING CONTROL

Network Segmentation - Purdue Model

- Terminates connections from zone to zone, level to level
- Only allow legit traffic through
- Many old switches support Access Control Lists which can be configured close to the destination to blocks illegitimate source IP addresses
- Principal of least route (similar to principal of least privilege)

ECL
ENGINEERING CONTROL

Demo – Attacking the ICS



Mitigations

Individually:

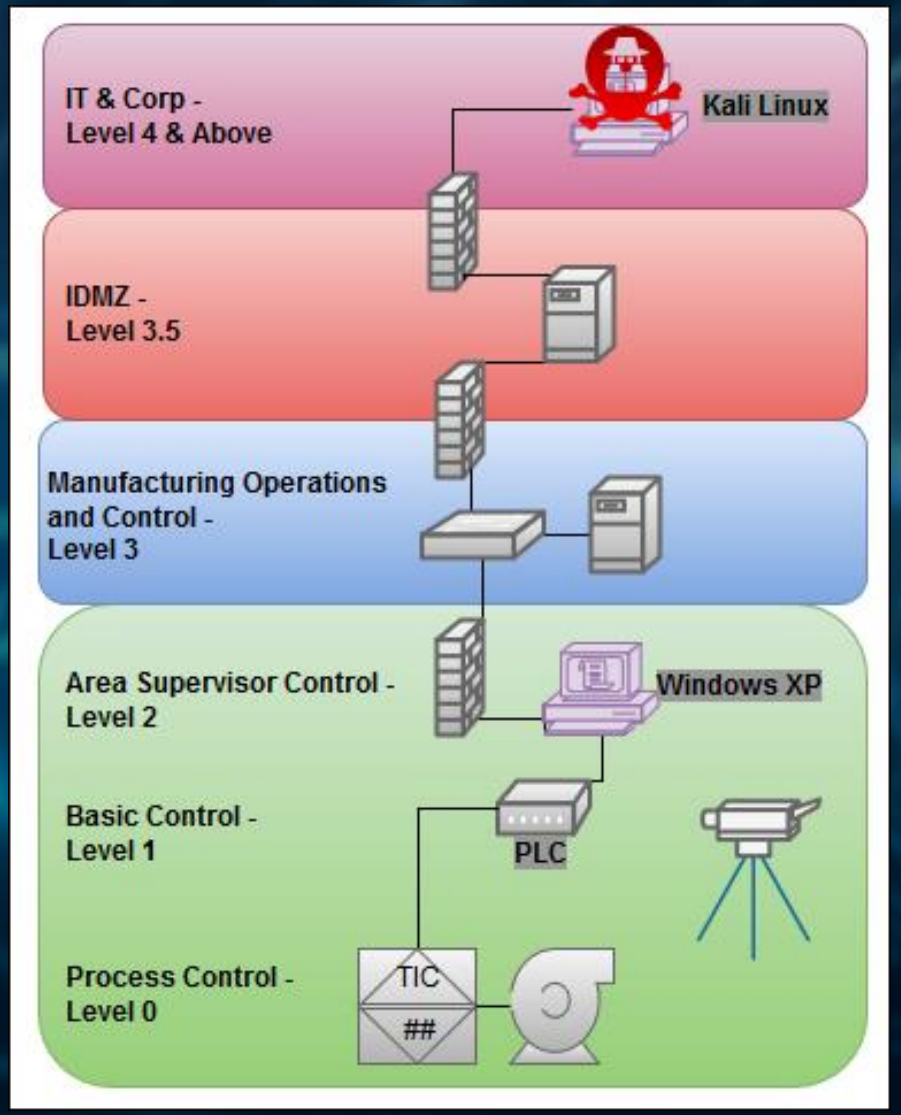
- Anti-Malware, not that effective (PPE)
- Patching, Update O.S. , Update PLC Firmware
- Network Segmentation, Principal of least function (route and privilege)

All together:

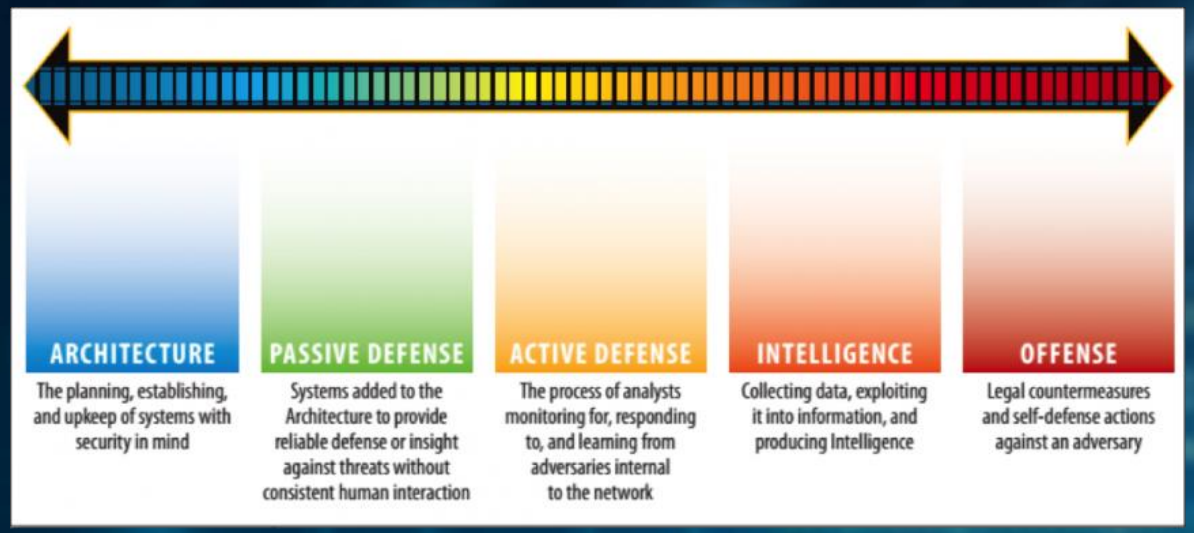
- Defence in-depth, very effective at mitigating risk and likelihood of compromise.
- D.i.D. Implementation can be difficult and dependant on plant shutdown
- First-Steps is a Risk Assessment, Audit or Gap Analysis. Essentially find where you a vulnerable

ECL
ENGINEERING CONTROL

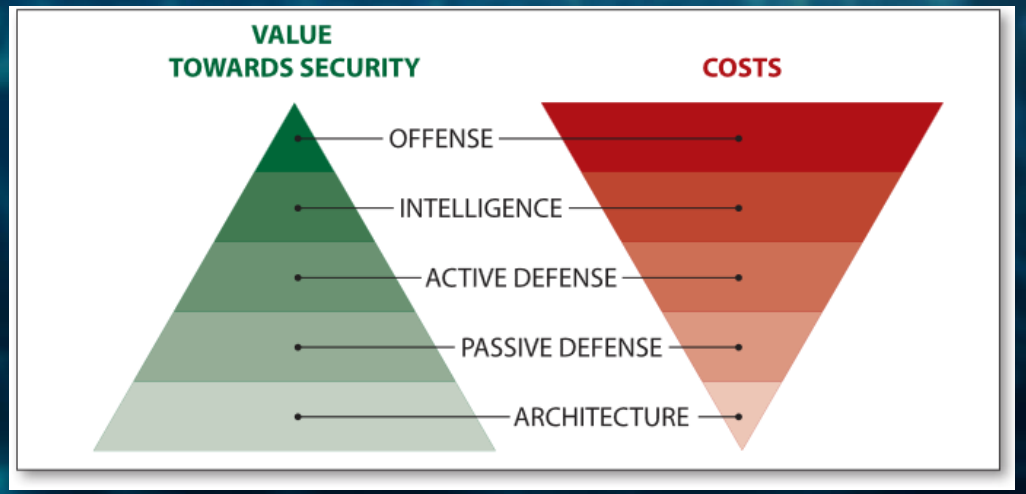
Mitigations – Defense in-depth



Effectiveness vs Cost



- Network Segmentation
- Patching, Anti-Virus
- Monitoring, Incident Response



ECL
ENGINEERING CONTROL

Advanced / Active Defence

- Host Baseline – (application white listing, known software executables. Known executables in RAM)
- Network Baseline – who talks to who and with what ?
- A good time to conduct a penetration test is during a cFAT
- Monitoring: log what you can and respond to the alerts generated
- Assemble an Incident Response Team
- Training is crucial for success of any defensible position, so are 'drills' and table top exercises

ECL ENGINEERING CONTROL

YouTube Demonstration

https://www.youtube.com/watch?v=jdESl85ocKQ