



**Regional Forum on Cybersecurity in the Era of Emerging Technologies
&
the Second Meeting of the “Successful Administrative Practices”-2017
Cairo, Egypt 28-29 November 2017**

Critical Infrastructure Protection (CIP)

by

Mohamed Abd El Haleem

CCISO, CEH, CHFI, ECSA

**ISO27001LA, ISO PENTEST, ISO/IEC 38500 Lead
Corporate Governance Manager, CERTIFIED Lead
SCADA Security Professional**





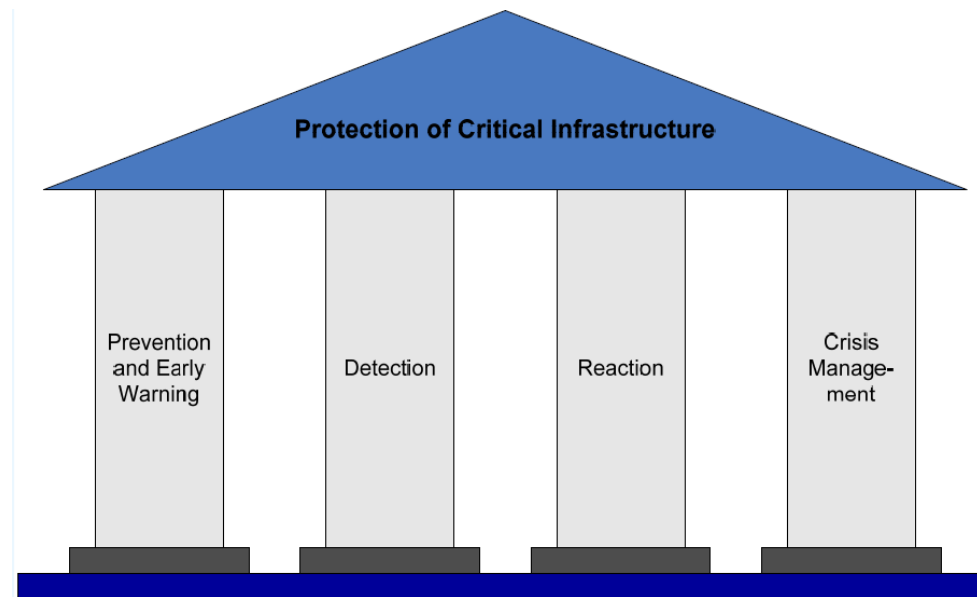
Critical Infrastructure Protection (CIP)





Critical Infrastructure Protection (CIP)

Critical infrastructure is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens.





Defining Industrial Control Systems





Defining OT and IT

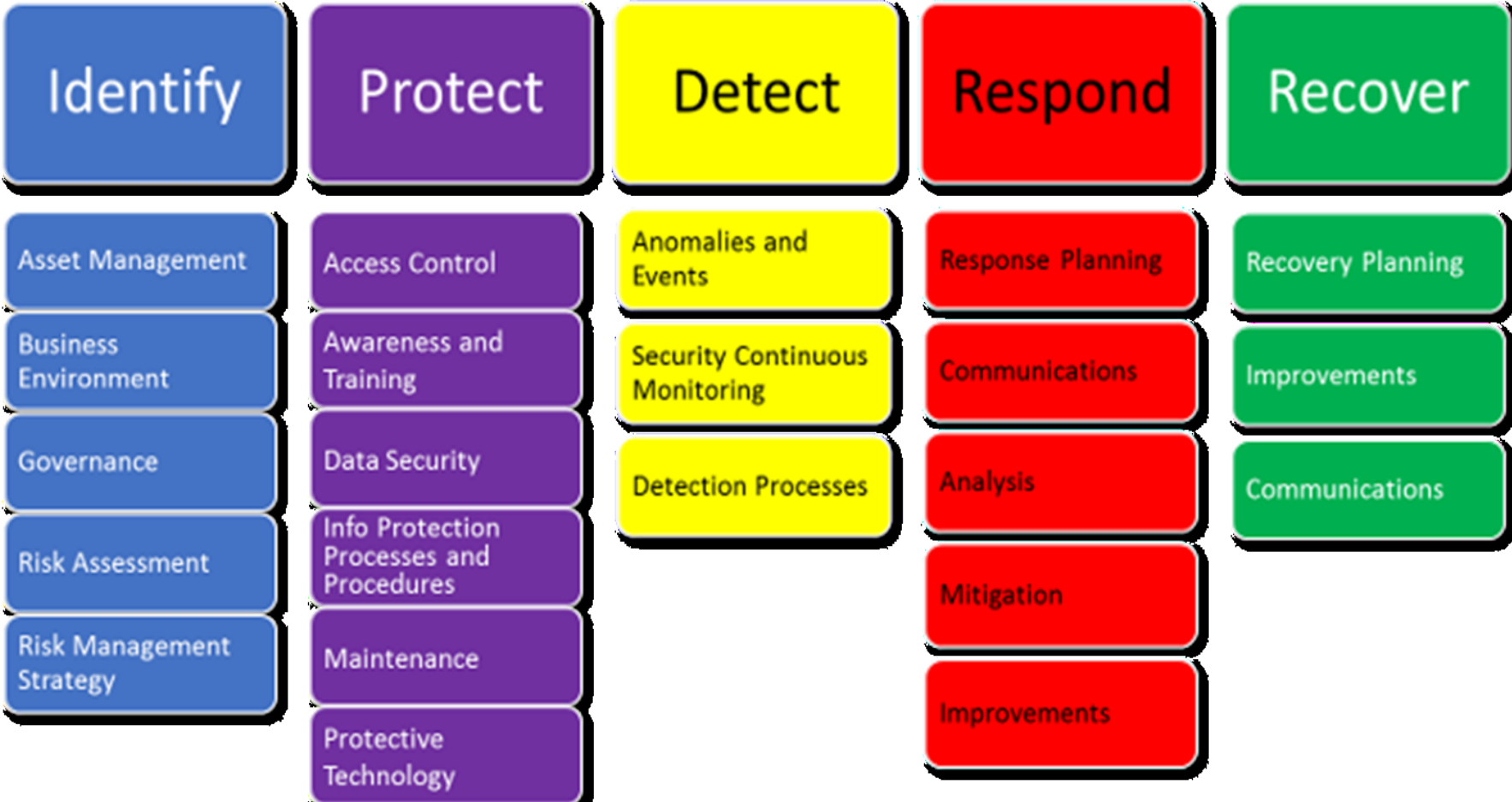




NIST CyberSecurity Framework



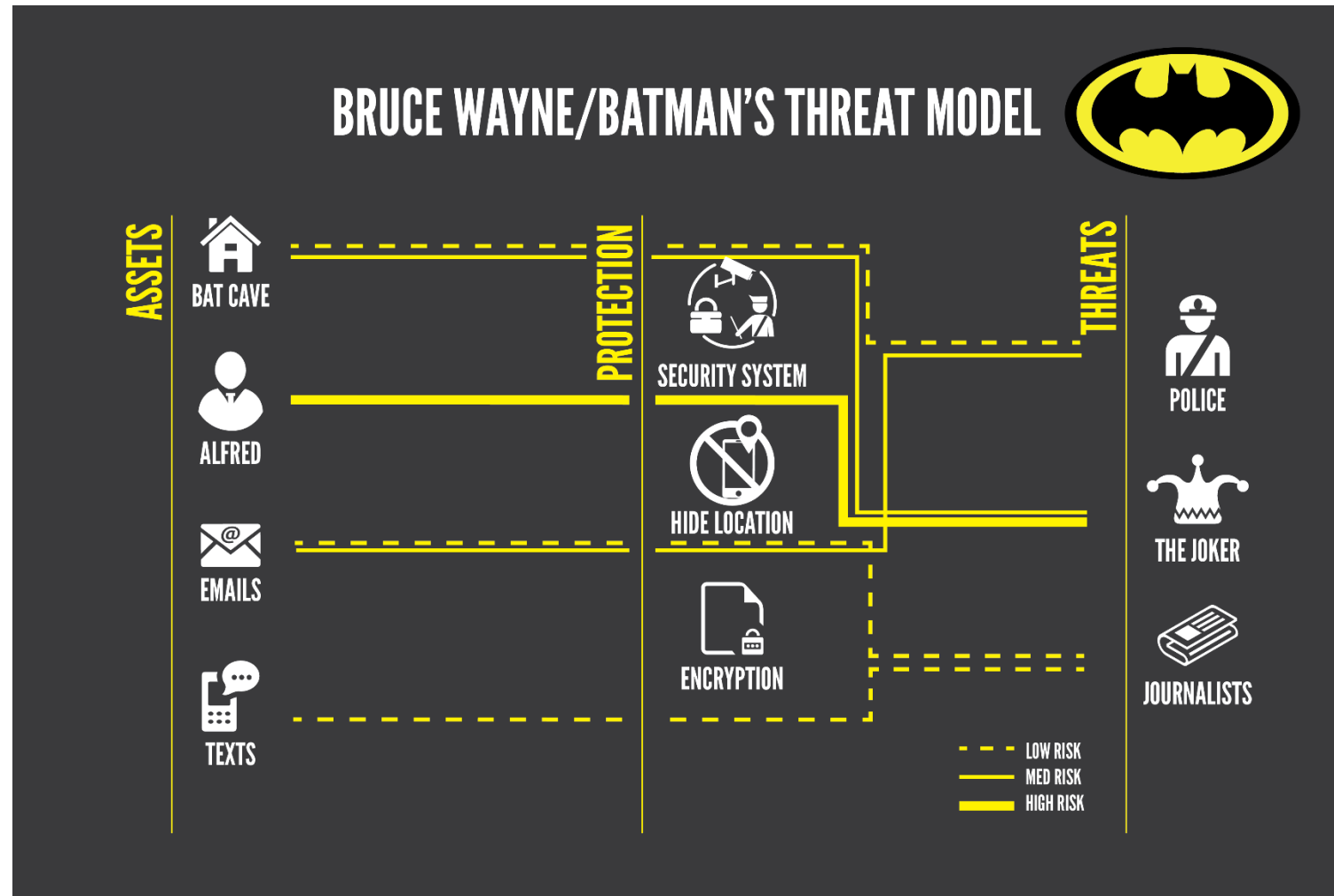
NIST Cyber Security Framework





Top Practices To Secure The Industrial Control System (ICS)

1. Threat Modeling





4. Honey pots





5. Vulnerability Management



8. Configuration Hardening





7. Source Code Review



10. Strong Authentication





9. Encryption







Mohamed Ahmed Abd El Haleem

Email: mohamedhaleem2@msn.com

Mob.: 0100 440 2408

Linkedin: Mohamed Abd ElHaleem

