Fundamentals of Resilient Cybersecurity

Franklin Witter, CISM, CISSP
Product Manager, Active Threat Analytics
June 2016

Critical Must-Haves

1. Penetration Testing & Vulnerability Management Program
2. Accurate inventory of systems and applications
3. *Network Segmentation (Principle of Least Privilege)*
4. *Effective Patch Management (OS and Applications)*
5. *Secure Engineering and Coding Practices*
6. *Skilled, Well-Trained Staff (Not just in security)*
7. *Written and Well-Rehearsed Incident Response Plan*
8. *24x7 Security Operations*

Moving Beyond Fundamentals

1. Strong Authentication (Two-factor or password vaults)
2. User and Network Behavior Analytics
3. Incident Response Automation
4. Integrate Security Risk Management into Enterprise Risk Management