Cyber Security Planning – Managing Tools, Talent & Technology

PTC 2020
Cyber Security Planning
Managing Tools, Talent & Technology

• Budgeting for infosec beyond just standard IT is difficult and can be expensive

• Hiring, training and keeping a talented infosec person is hard

• Technology is expensive – multiple point products may be required to meet your regulatory, compliance or security needs. How do you pay for and manage them all?
Planning & Prioritizing – Tools

“Must have” tools to be successful (CIS Controls v7.1 - basic)

• Accurate inventory of hardware and software assets
• Vulnerability management
• Secure configurations of all assets (“Golden Images”)
• Maintenance, monitoring and analysis of audit logs (SIEM)
• Quality Backups

Match technology and talent

• Connect Tools and Talent as part of the picture of success
• Businesses need a technology roadmap
• Roadmaps evolve over time to meet business objectives
• Make smart investments in technology that your team can support
  – Don’t buy so many tools that your team is focused on tool management and not CIA triad
  – Technology investment does not equal security
Cyber Talent

Two opposing (or complementary?) approaches

- **Embrace Turnover**
  - Robust new hire training
  - Solid, documented procedures and policies
  - Industry standard (or easy to use) toolset

- **Retain the talent you have through Career development**
  - Make a list of all the things your Infosec team should learn or know
  - Link these requirements to the roles in your plan
  - Allocate portion of your budget for training and certifications

- **Find a partner that can fill your gaps**
  - Utilize annual retainer, project based work, or managed security services
  - Managed Services
In Conclusion

• Focus on the tools that align with your security goals & budget

• Invest in your talent through training and career development

• Develop a technology roadmap that supports the business
Further the discussion with us in THE HUB