Ten “Easy” Steps to Building a Successful Extended Security Team
EXTENDED – The What and The Why

- ex.tend.ed (adjective) - made larger, greater coverage, greater impact
- Force multiply impact of your security team
  - Security champions/advocates
  - Security Architects
  - Security Leads
- Shared goals and responsibilities
- Extended accountability and visibility
In an Ideal Business World...

...Sure let me pull a full million off the tree next door
But in the Real Business World...

Hard work, creative prioritization, limited resources and limited funds

BUT IT’S POSSIBLE!
Build Your Team Within 180 Days

- Within 30 days (Steps 1 & 2)
  - Identify Need & Frame the Drivers

- Within 90 days (Steps 3-5)
  - Develop Roles & Responsibilities
  - Package the Message to Leaders
  - Identify Potential “Recruits”

- Within 180 days (Steps 6 & 7)
  - Identify/Develop Training Material
  - Deliver Effective Training

- Within one year (Steps 8-10)
  - Measure their Effectiveness
  - Cultivate & Keep Them Engaged
  - Grow the Pipeline
Step One: Recognize the Need

Is the team overworked/frustrated?

Is your risk increasing?
Step Two: Frame the Drivers

- Visibility
  - Do you know what you have (systems, services, providers, etc.)?
  - Do you know which of these provides the most value to your business?

- Accountability
  - Do you have someone accountable for security of each?

- Measurability
  - Can you measure current risk posture state or security maturity?

- Strategy
  - Does security have a seat at the table?
Step Three: Develop Roles & Responsibilities

Security Leaders
- Ensure end to end security for (service, systems, applications, providers)?
- Raise awareness of security in area.
- Ensure sufficient security “doers”.
- Develop security strategy for area.
- Ensure security has seat at table.
- Message up to leadership.

Security “Doers”
- Perform security architecture & deployment reviews.
- Complete security artifacts (threat models, data flow diagrams, architecture reviews).
- Act as security SME to clients for area.
- Continuous learning in security arena.
- Develop trusted partnerships.
Step Four: Package the Message to Leaders

- Don’t use FUD, but share real risk exposure and incidents.
- Emphasize partnership with security team.
- Demonstrate value add – business enablement and cost reduction.
- Test the waters with a few key leaders.
Step Five: Identify Potential “Recruits”

Who Are the Ideal Candidates?

- Have visibility within the org.
- Can influence key people.
- Understand services & offerings in area.
- Have passion for security & learning.
- Have cycles to do required work.
- Have support from senior management.
Step Six: Identify/Develop Training Material

Technical Knowledge
- Security foundations
- Common attacks
- Defense in depth
- Architecture reviews
- Threat modeling
- Risk modeling

Process Knowledge
- Roles and responsibilities
- Security policies
- Governance requirements
- Data classification
- Privacy concerns
Step Seven: Deliver Effective Training

- Hold in person and video bridge.
- Provide sufficient food/munchies/drinks.
- Use internal resources to deliver.
- Make training days manageable.
- Allow ample time for discussions & networking.
- Keep class engaged, ask questions.
- Have review session and test at the end.
- Keep materials updated and relevant.
Step Eight: Measure Their Effectiveness

Measure the Right Things

- Coverage (leaders & doers) per area
- Growth (knowledge) of teams
- Risk posture for area
- Governance process compliance levels
- Consistent seat at table

Keep it Reasonable

#RSAC
Step Nine: Cultivate & Keep Them Engaged

Ownership - Passion – Growth - Results

- Provide ongoing training.
- Provide growth opportunities.
- Involve in strategy planning.
- Involve them in training others.
- Mentor them to mentor others.
- Provide internal and eternal visibility.
- Provide rotation opportunities.
Step Ten: Grow the Pipeline

The Challenge

The 2014 Cisco Annual Security Report estimated that by the end of 2014 the industry would be short more than a million security professionals across the globe. Today the prediction is that by 2017 this gap will grow to 2 million workers worldwide.

A Solution

- Get backing from senior leaders.
- Socialize testimonials from extended team.
- Demonstrate results by having extended team.
- Target Managers, Service Owners, Architects, Engineers, New Hires.
- Brand security as the coolest job in the company.
Thank You