Starting from Scratch

Building a Security Program From the Ground Up

@HomeBrewedSec

#InfoSecIn365

Phases

Phase 1 *Planning and Discovery*

Phase 2 *Analysis and Documentation*

Phase 3 *Mitigation and Remediation*

Phase 4 *Looking Forward*

#InfoSecIn365

Phase 1
Planning and Discovery

Discovery

- Framework
  - ISO 27000 *($)*
  - NIST CSF
  - CIS Controls (formerly SANS Top 20)
- Resource Assessment – Financial, Infrastructure, Technical
- Asset Discovery – Software and Hardware
- User Education
  - Phishing Simulation
  - Surveys/Quizzes (Staysafeonline.org)
  - Use results for targeted user training

#InfoSecIn365

Threat Modeling

- Know what you're protecting. Know what you're protecting against

- Risk Assessment + Business Impact Assessment
  - Estimate what happens to the business if X happens, and the likelihood of X happening

- Red Team Simulation

Talk with Management

- Understand Business Objectives
  - Evaluate Disaster Recovery capabilities vs. management expectation
  - Data Classification
  - Security Policies
- Increase buy-in
  - Pitch security as a sales tactic
- Discuss potential costs / resource issues
  - Just because little to no money has been spent, that is not the expectation going forward

#InfoSecIn365

Phase 2
Analysis and Documentation

Vulnerabilities

- Assessment
  - Implement prior to patching to show reduction in vulns from patching
  - OpenVAS (with VulnWhisperer (ELK))
  - Generate differential reports
  - Shodan lookup for external ports
- Patching
  - Automated for endpoints, manual for servers
  - Gather team from IT for server patching
  - WSUS can be high-maintenance if you don't have experience
  - Every MS(S)P will have a patching software

Incident Response Prep

- Policies/procedures
- Breach Reporting
  - At what point
  - Compliance requirements?
- Establish CERT Team
  - Legal/HR/PR/Management/Infosec/IT

#InfoSecIn365

Change Management

- Not necessarily your job…but it will be if it doesn't happen
- Even track changes that you don't think require approvals
- Tools
  - Excel
  - Intranet/SharePoint
  - Google Form
  - Helpdesk

#InfoSecIn365

Phase 3
Mitigation and Remediation

Least Privilege

- Discovery
  - PowerShell
  - Talk to people
  - Bloodhound
- AD Admin Delegation
- ProcMon for removing Local Admin
- Reduction of privileged AD accounts

#InfoSecIn365

Easy Wins

- Firewall rule closures

- Session lockout

- Pre-logon advisory

- Add encryption into PC build checklist

- Account Auditing
  - Based on last logon + work with HR
  - Change service account and admin passwords

#InfoSecIn365

Replacement/Renewals

- Good chance to increase security with easy wins
- NGAV
  - Does more than just AV, not much more $
  - "Poorman's App Whitelisting", Removable Media Control
  - Bit of an upfront effort
- Network refresh
- WAPs with RADIUS
- LAPS

Phase 4
Looking Forward

Measure Progress

- Distribute survey
  - Measure user pain/perceived improvements
  - Allow Suggestions
  - Self Assessment
- Differential reports
  - Perform another Gap analysis
  - Vulnerability Scan
  - Redistribute survey from beginning to measure improvement in user awareness

#InfoSecIn365

Budget Preparation

- Set Priorities based upon findings in last slide
- Re-evaluate threat model, risk assessment
- Revisit MSSP for SOC
- Suggestions
  - MFA
  - Network overhaul (chances are you have a flat network with L2 switches)
  - Suggestions from Renewals/Replacements
  - Principle of least Functionality / Hardening
  - SIEM
  - (N/H)I(D/P)S

Talk with Management

- Present Budget
- Infosec as profit center
- Present % compliance improvement goals
- Present differential reports
- Explain advanced concepts

tl;dr

- Set priorities based upon business objectives
- Threat model all the things
- Discover all the things
- Educate all the users
- Backup all the things
- (Don't necessarily) open source all the things
- Buy all the things … eventually

#InfoSecIn365

Appendix: Resources

- Framework
  - ISO 27000 *($)*
  - NIST CSF
  - CIS Controls (formerly SANS Top 20)
- Phishing Simulation
  - Knowbe4 *($)*
  - PhishMe *($)*
  - SANS Securing the Human
- Surveys/Quizzes
  - StaySafeOnline.Org
- Asset Discovery
  - NMAP
  - Vulnerability Assessment System (VAS)
  - Active Directory
  - Microsoft Baseline Configuration Analyzer

- Threat Modeling
  - US-Cert
  - Threat Exchange
- User Education
  - StaySafeOnline.org
  - SANS Securing the Human
- Security Policies
  - SANS
  - Charles Cresson *($)*

#InfoSecIn365

Appendix: Resources (cont.)

- SIEM
  - Elastic Stack
- Vulnerability Assessment
  - OpenVAS + VulnWhisperer
- NIDS
  - Bro
  - Suricata / Snort
- HIDS
  - Osquery
  - OSSEC / Wazuh

- Incident Response
  - *The Hive*
- Patching
  - WSUS
  - Comodo
  - Rudder
- AD Discovery
  - Bloodhound
- Applocker
  - AaronLocker
- Symon
  - SwiftonSecurity
  - Red Team Simulation
    - Red Canary Atomic Red Team

#InfoSecIn365

Oh $#*7

I have to do WHAT?!

365 days to build a security program

Slides
homebrewedsec.com/talks/

Questions
@HomeBrewedSec
#InfoSecIn365