Council Chairs

Alen Kirkorian

• Currently at Department of State, as the Division Chief for the Office of Innovation, Strategy, and Security
• Formally a Chief Information Security Officer (CISO) at the Overseas Private Investment Corp (OPIC), and Deputy CISO at the United States Agency for International Development (USAID)
• Actively chairing the Small and Micro Agency community for 7 years.

Dan Jacobs

• Currently GSA’s Cybersecurity Coordinator
• Also supporting GSA’s Centers of Excellence (Cyber COE)
• Formerly Cloud Security Architect (DOS), SISO at Defense Media Activity, Director of APG Network Enterprise Center, RCERT-Europe Director
• Supporting the SMAC for 4 years
Agenda

• Introduction to SMAC
• Collaboration
• Challenges
• Solutions
• Ideas on the way forward
Introduction

• What is the SMAC?
  • Grass-roots group of security professionals focusing on security issues affecting government agencies/corporations with fewer than 2000 people
  • Consists of 158 different government agencies represented by >200 CIOs, CISOs, and security practitioners
  • Federal heavy (few contractors, few state/local/tribal)

• Primary Goals
  • Collaboration
  • Training and education
  • Influence government-wide decision making
Collaboration Mechanisms

- **Knowledge Management**
  - Max.gov SMAC page (calendar events, presentations, papers, etc)
  - SMALLAGENCYCISO email distro list
    - Security Q&A, support and solutions, trends, governance, etc

- **Bi-Weekly Lunch and Learn sessions**
  - WebEx-based vendor spotlight for new/interesting security solutions
  - Format is 45 min for technical presentation, 15 min of Q&A
  - Wide range of topics covering most security aspects

- **Bi-Monthly Face-to-Face Meetings**
  - Hosted by different agencies across NCR
  - Provides 5-6 different sessions focused on current security issues relevant to Small and Micro Agency CISOs
  - Presentations regularly provided by OMB, DHS/CISA, and GSA
Collaboration Mechanisms Cont.

- **Surveys**
  - Anonymous
  - Cover various security concerns, issues, etc
  - Results help provide realistic picture
  - Anonymized and shared with the entire SMAC community
  - Can (and does) inform gov-wide decision making
Challenges

- All the security requirements, none of the funding
- Acquisition challenges (scale directly affects price)
- Perception
  - Small Agencies are insignificant
- Kitten herding
- Legacy security mindset
  - “FedRAMP and forget it”
- Commonality problem
  - Common controls/governance/solutions/audits
  - Answer is to replicate solutions 158 times... not viable
  - The solution is clear... and impossible (apparently)
Solutions

• All roads lead to consolidation
  • CDM is a start
  • SOCaaS will really help
  • Shared/integrated threat feeds are +
  • SOAR and AI-powered capabilities are ++
• The best security solution isn’t a security solution
  • Enterprise as a Service
    • Transport (e.g. DCNet + ZTN/SDN)
    • Desktop and collaboration software (e.g. O365, GMail)
    • Storage (cold too!)
    • Web presence (e.g. Federalist)
    • MDM
    • Single, centrally-managed security (agency inherited)
    • CICD pipelines
    • SLA-driven performance and accountability for agencies
Way Forward

• Ideas on the way forward
  • Smalls are government too (deal with it)
  • The problem is not a technical one, it's a human one
Questions

Contact
Alen Kirkorian
kirkoriana@fan.gov

Dan Jacobs
daniel.jacobs@gsa.gov

5/8/2019  Small and Micro Agency CISO Council