SIEM @ CAP

Nick Levay <nlevay@americanprogress.org>
Information Security and Operations Manager

The Environment

- High Visibility
  - Constant media attention
  - Frequent high profile visitors
    - Bill Clinton, Joe Biden, Janet Napolitano, Tony Blair, et cetera
- Threat Rich
  - Foreign Espionage Target
  - High Volume of Drive-By attacks (just like everyone else)
  - High personnel turnover
    - Over 100% a year … interns, interns, and more interns!
- Target Rich
  - Enterprise office environment
  - High volume web sites
    - thinkprogress.org ~ 3M visits/month
  - Multiple partner organizations sharing facilities
    - National Security Network, American Constitution Society, Century Foundation, Enough Project, et cetera

Key Elements of Security Strategy

- Perimeter filtering and logging
  - Inbound, Egress, Internal
- Endpoint
  - Traditional Anti-Virus is useless
  - White-listing is the future^H^H^H^H^H^H^Hnow
- Update Management
  - Security updates **must** be applied < 48hr
- Vulnerability Management
  - Vulnerability-centric
- Counter-Intelligence
  - Threat-centric

Log Management and Review is CRITICAL

- APT focuses on getting legitimate user credentials
  - Know who is targeted
  - Review all access by targeted individuals
- Develop indicators you can use
- Speed and ease are mandatory
  - The X-Ray Operator Syndrome, your 15-minutes of fame
  - Review capability is more important than alerts
  - Many reports are only run once
- Compliance != Secure
  - Your K-rad SEIM Dashboard doesn’t matter either…

Questions?

Nick Levay
<nlevay@americanprogress.org>