Best of Both Worlds

Blending Tactics from the Public and Private Sectors
Disclaimer

While this talk will briefly touch on security concepts and how they relate to security controls, the focus is on security management and forensic capabilities for defense. The opinions I present are mine only and do not reflect on my current or previous employers in any way, shape, or form and have no relation to any real life events or incidents.
Josh M. Bryant
Director of Technical Account Management

Master Sergeant

183D WING
Public vs Private

- Military
- Federal Government
- State Government
- Local Government

- Corporations
- Non-Profits
- Education
Public ➔ Private

People ➔ Technology

Process
Strengths

Public Sector
- Communication
- Structure/Discipline
- Documentation
- Training

Private Sector
- Agility
- Innovation
- Talent
Weaknesses

Public Sector
- Rigid/Slow
- Stagnant
- High Turnover

Private Sector
- Siloed
- Disorganized
- Budget
What’s the **SECRET**?

Military Grade…

- …Hardware? **MYTH BUSTED!**
- …Software? **MYTH BUSTED!**
- …Encryption? **MYTH BUSTED!**
- Basic Cyber Hygiene
Back to Basics

CIS Top 20

1. Inventory and Control over Hardware Assets
2. Inventory and Control over Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Endpoints
6. Maintenance, Monitoring, and Analysis of Audit Logs

14 more controls at:
https://www.cisecurity.org/controls/cis-controls-list/
A Blended Example
Unmanageable, undefendable.
Focus Areas
Not so different after all…

Public Sector
• Mission Critical

Private Sector
• Business Critical
Manageable, defendable.
Defenders can live off the land too…

```
gwmi -Class win32_process -Property * | FL ProcessName,ProcessID,CommandLine,Path


```
## Combing Strengths

### Overcoming Weakness

<table>
<thead>
<tr>
<th>Public Sector</th>
<th>Private Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Communication</td>
<td>• Siloed</td>
</tr>
<tr>
<td>• Rigid/Slow</td>
<td>• Agility</td>
</tr>
<tr>
<td>• Structure/Discipline/Documentation</td>
<td>• Disorganized</td>
</tr>
<tr>
<td>• Stagnant</td>
<td>• Innovation</td>
</tr>
</tbody>
</table>
Takeaway Challenges

• Be a Leader, no matter what your position/title is.
• Identify Strengths and Weaknesses.
• Learn from others.
• Have a Mission Statement.
• Master core concepts, but don’t be afraid to fight for tools that help the mission.