The Business of Battle Readiness: Over-the-Horizon Threat Management for Companies and Agencies

+ Roland Cloutier
ADP Staff Vice President, Chief Security Officer
A Responsibility to Protect
Historical Cyber Defensive Operation Practices
Imagine fighting from this position
3 Incredible Shifts
Since the Rainbow Series

The Interconnected Mission Space
The Business of the Black Cyber World
Speed of Technical Manipulation
The Real Battle Field
Over the Horizon Threat Management Pillars

• Threat Transparency
• Threat Impact Analysis
• Threat Decision Support & Action
Over the Horizon
Threat Transparency

Who is harming who?
Industry / Agency Alignment
Tactics, Techniques & Procedures
Impact Analysis

1. Know Your Business
2. Risk Management
The Success of their Business
The Success of your “Security” Business

- Business Process Documentation and Threat Analysis
- Threat Surface Acknowledgment – Knowing Your Limits
- Creating Your Sense of “Normal”
Defining the What If: Risk Articulation

Assessment & Validation
- Enabling the “What If” – Path Vector Analysis etc
- How Big is My Problem
- Probability Alignment

Risk Articulation
- Defining Impact
- Make it Repeatable
- Automate it
Decision Support – Making Your Horizon Actionable
Battle Space Decision Support

Mature Your Prioritization Process

- Line Level Actionability
- Transparency: The What & Why
- Documented and Easily Followed
Advanced Response

Move the Cheese Methodology – Willful Control
Obfuscation

Partner Selection

Burstable Cloud
Don’t Go It Alone

Incident Response
Threat Management
Technical Specialties
Law Enforcement & Law Firms
Opps; I Changed it again 😎
The Cloud is Your Friend

- Attacking the Defenders
- Don’t Size for “The Big One”
- Shared Response Capabilities
Enabling The Next Generation Defender
Advanced Condition Analytics

Collection and Expertise – Next Generation Security Defense

Security Intelligence Big Data Platform Force Multiplier

<table>
<thead>
<tr>
<th>Cyber</th>
<th>Business Process Protection</th>
<th>Response Intelligence &amp; Automation</th>
<th>Assessment and Assurance</th>
<th>Investigation</th>
</tr>
</thead>
</table>
Getting There:
Progressive Improvement Through Action

- Take Inventory
- Establish Legal Alignment
- Create Your Business View
- Develop a Core Big Data Plan
- Prioritize on Prevent, Detect, Contain, Response
Questions?