Moving Up the Maturity Curve
The Sisyphean Task
INTRODUCTION

Jamie Hari - Director of Cloud & Security

- Managed Security Services Provider x 2
- DNS Security Vendor
- Video Surveillance & Analytics Vendor
- Enterprise Software / Financial / Telecom
INTRODUCTION

Jamie Hari - Director of Cloud & Security

• Technology Geek
• Comic Book Geek
• Music Geek
• Security Geek
10.4M Fiber Miles
124,000 Route Miles
49 zColo Data Centers
391 Markets Served
SECURITY MATURITY

Defining Security Maturity
SECURITY MATURITY

Maximize ROSI
SECURITY MATURITY

Technology Is Not the (Only) Answer

[Diagram showing the interconnection of People, Process, Culture, and Technology]
SECURITY MATURITY

Holistic Thinking
SECURITY MATURITY

Back to Basics

CIS Critical Security Controls - Top 20

1. Inventory of Devices
2. Inventory of Software
3. Secure Hardware & Software Configurations
4. Vulnerability Assessment
5. Controlled Admin Privileges
6. Logging
7. Email and Web Protections
8. Malware Defense
9. Control of Network Ports & Protocols
10. Data Recovery Capability

11. Secure Network Configurations
12. Boundary Defense
13. Data Protection
14. Need-to-Know Access Control
15. Wireless Access Control
16. Account Monitoring & Control
17. Security Skills Training
18. Application Software Security
19. Incident Response and Management
20. Penetration Testing

• Exhaustive?
• Up-to-Date?
• Automated?
HOW TO THINK ABOUT ROSI

ROSI Calculators

SAVINGS POTENTIAL

<table>
<thead>
<tr>
<th></th>
<th>Factor</th>
<th>Current</th>
<th>Target</th>
<th>Savings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduction in costs of incidents (monthly)</td>
<td>10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Reduction in costs of problems (monthly)</td>
<td>10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Reduction in costs of open problems (monthly)</td>
<td>10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Reduction in cost of prevented incidents (monthly)</td>
<td>10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Reduction in cost of TIA violation (monthly)</td>
<td>10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Reduction in cost of unauthorized Co- (monthly)</td>
<td>10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Reduction in cost of changes (monthly)</td>
<td>10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Reduction in cost of unauthorized changes or rework (monthly)</td>
<td>10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Reduction in cost of incidents incurred by changes (monthly)</td>
<td>10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Reduction in costs of new changes (monthly)</td>
<td>10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>TOTAL (monthly)</td>
<td>10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

Factor - savings factor, i.e. targeted savings expressed in percentage. Change savings factor (entered in percentage) according to expected results.
Current - Current Costs Calculated.
Target - Calculated Target costs.
Savings - Calculated savings after ITIL processes and functions implementation.

Tell Us About Your Current Organization

1. Alerts per Week - Average Organization
2. False Positive Rate
3. Alert Capacity per Week
4. Average Time to Investigate an Alert (Hours)
5. Average OFEX to Investigate an Alert

<table>
<thead>
<tr>
<th></th>
<th>Standard Deployment</th>
<th>Offsite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average time to identify alert that matter</td>
<td>304 Minutes</td>
<td>4 Minutes</td>
</tr>
<tr>
<td>Annual operational expenditure to process all alerts</td>
<td>$12,022,000</td>
<td>$1,596,000</td>
</tr>
<tr>
<td>Annual operational expenditure to process all false alerts</td>
<td>$10,441,000</td>
<td>$13,860</td>
</tr>
<tr>
<td>Alert prioritization</td>
<td>None</td>
<td>Current Events / Alerts TAP/Pete/Arts/AT/119PC</td>
</tr>
<tr>
<td>Annual OFEX savings with inline deployment</td>
<td>$0</td>
<td>$1,205,360</td>
</tr>
</tbody>
</table>
“It's a good idea in theory, but it's mostly bunk in practice. [...] The key to making this work is good data.”
- Bruce Schneier
HOW TO THINK ABOUT ROSI

Beware the Cost of Free
ACCOUNTABILITY & RESPONSIBILITY

Consolidate Accountability
ACCOUNTABILITY & RESPONSIBILITY

Define, Educate, Reinforce

<table>
<thead>
<tr>
<th></th>
<th>Executive</th>
<th>Finance</th>
<th>Account Lead</th>
<th>Director</th>
<th>Production</th>
<th>SAE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business case</td>
<td>R</td>
<td>A</td>
<td>C</td>
<td>I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance Plan</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementation</td>
<td>C</td>
<td>I</td>
<td>A</td>
<td></td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Launch</td>
<td>I</td>
<td></td>
<td>R</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event</td>
<td>R</td>
<td>I</td>
<td>A</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video Release</td>
<td>I</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SECURITY PROGRAM ASSETS

Security Program Assets

- Security Team Skills Matrix
- IT / Internet AUP
- Asset Summary
- Application List
- BC/DR Plan

- Data Retention Policy
- Network Architecture Diagram
- Recent Vulnerability Assessment
- List of Applicable Compliance Standards
PASSWORD POLICY

Password Reuse

55%
Rethink Password Dogma

**PASSWORD POLICY**

Through 20 years of effort, we’ve successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.
PASSWORD POLICY
Password Management
ROLE-BASED ACCESS CONTROL

Drive Efficacy, Reduce Human Error
SECURITY INCIDENT RESPONSE PLAN

Define, Educate, Reinforce

- Identify and continually monitor:
  - Existing skills, missing skills, and single points of failure
  - Part of the documented RACI
  - Improved through measured repetition, just like fire drills
Your Security Includes Their Security
SECURITY CULTURE

Resting Suspicious Face

SUSPICIOUS ALPACA KNOWS WHAT YOU'RE UP TO!
Many modern applications support it
Simplified MFA tools, like Authenticator, provide improved UX
Combined with SSO, further reduces password challenges
ATTACK SURFACE

Reduce Your Attack Surface

- Aggregate Internet ingress / egress
  - Less to manage, easier to monitor
- Remove bloatware from default system images
  - Less to patch, less to exploit
- Software
  - Deprecated / Custom APIs
  - Admin interfaces / Login and authentication entry points
Thank You