Metrics: Beyond ROI

Shawn Chakravartty & Kevin Tyers
SANS SOC Summit 2015
To maintain privacy for our current and previous employers, numbers have been changed.
Who we are
Shawn Chakravarty
Sr. Manager of Security Incident Response
Kevin Tyers
Information Security Engineer
Concepts
Concepts

High Level
- What does your business find most valuable?
- Does ROI always have to be represented in money?
- Do you have a top to bottom metric strategy?

Technical
- Do you have the means to gather metrics?
- Do you visualize your metrics?
- Are you consistent in your data collect?

“What's measured improves”
Peter F. Drucker
Value Scale

Different Metrics mean Different Things to Different People at Different Levels
C-Level and Board Metrics

(Or Why are we paying for this?)

What is valuable for the business?
How do we measure this?
How much does one $x$ cost to protect $y$ units of value?
C Suite - Aggregate Available Resources

| Var | R = RAM  
|     | BW = Bandwidth  
|     | C = CPU  
|     | A = Aggregate Available Resources |

| Eq | (R + (BW * .01)) * C = A |

| Ex | (10 + (1 * .01)) * 2 = 20.02 |
C Suite - Aggregate Available Resources v. (P)TPV
Director and VP
(Or how do we plan?)

How do we enable the business?
What can we measure for guidance?
Where are resources best spent?
Force to Load - Basic

Var
M = Mean time to restore
A = Analyst
T = Tickets
H = Hours

Eq
(T * M)/(A * H) = Force to load (F)
F = 1.0 is perfect

Ex
(500 * 4)/(50 * 40) = 1.0 Perfect
(500 * 4)/(25 * 40) = 2.0 Need more resources!
(500 * 4)/(75 * 40) = .67 Need more work!
Force to Load - Advanced
Weighted ticket types

\[ \frac{(T1 \times M1) + (T2 \times M2) + \ldots + (Tn \times Mn)}{(A \times H)} = F \]

**Ex**

\[ \frac{(25 \times 8) + (300 \times 4) + (200 \times 0.5)}{50 \times 40} = 0.75 \]
\[ \frac{(25 \times 8) + (300 \times 4) + (200 \times 0.5)}{25 \times 40} = 1.5 \]
\[ \frac{(25 \times 8) + (300 \times 4) + (200 \times 0.5)}{75 \times 40} = 0.5 \]
Force to Load: Visually

Force to Load

© 2015 PayPal Inc. All rights reserved. Confidential and proprietary.
Multi-tier Metrics
Force to Load

Director

- What are my budget needs?
- What is our security effectiveness?
- What does my threat landscape look like?

Manager

- Where is our time going?
- Where can we automate?
- What training do we need?
Managers
(Or how do we execute?)

Mgr

Encourage IC development
Addressing bad behaviors
Maximizing tactical capacity
Roadmapping: Tickets by Analyst Hours
Where are we spending our hours?
Roadmapping: Tickets Worked by Analyst

Who is working what issues?
Analyst/Individual Contributor
(Or how can I help?)

What am I contributing?
Where can I improve?
What is my career roadmap?
IC Knowledge Roadmap

Var

S = Subject
C = Comfort (1-10)
R = Required knowledge (1-10)

Eq

[C(S) < R(S) ] → Study(S)

Ex

C(Networking) = 8 – Learn as needed
C(Linux Admin) = 4 – Prioritize
# Knowledge Matrix

<table>
<thead>
<tr>
<th>Subject</th>
<th>C(S)</th>
<th>R(S)</th>
<th>Diff</th>
<th>Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking</td>
<td>8</td>
<td>6</td>
<td>+2</td>
<td>Learn as I go</td>
</tr>
<tr>
<td>Coding</td>
<td>8</td>
<td>3</td>
<td>+5</td>
<td>Pick up stuff as needed</td>
</tr>
<tr>
<td>Linux Admin</td>
<td>4</td>
<td>5</td>
<td>-1</td>
<td>Take the GCUX</td>
</tr>
<tr>
<td>Data Science</td>
<td>3</td>
<td>6</td>
<td>-3</td>
<td>Take Coursera Stats class</td>
</tr>
<tr>
<td>Documentation</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>Take a business writing course</td>
</tr>
<tr>
<td>Leadership</td>
<td>6</td>
<td>2</td>
<td>+4</td>
<td>Mentor new analysts</td>
</tr>
</tbody>
</table>
Thank you for your time

Questions?