Situational Awareness
A Discussion

Dean Weber
March, 2012
The Current Situation – take one...

- spending ...
- incidents ...
- financial losses ...
- overall risk grows ...
- resources applied grows but no real progress

The situation is getting more complex
The Current Situation – take two….

- **Attack**
  - Take down a utility
  - Disrupt a supply chain
  - Create financial mis-trust
  - **Success = Economic-Political-Military Dominance**
  - Steal intellectual property – the science
  - Create Disinformation
  - Find out how to attack critical infrastructures
  - **Success = Weaken your enemy**

- **Active Exploitation**
  - Reconnaissance
  - Mapping, Code Injection (moles in the network)
  - **Success = Find weaknesses**

- **Passive Exploitation**
The Current Situation – take three…our adversary is…

• **Invested (many months in the planning)**
  – Sophisticated
  – Stealthy
  – Coordinated
  – Stunning
  – Countered the counters

• **Means to OTHER ends**
  – Other high profile targets
  – Gain trusted access
  – Went directly to gain the trusted access
Current Situation – take four….

Cloud Computing
Mobility
Applications as a Service
...are compelling...

Security is getting harder...establishing situational awareness will be greatly more difficult.
Current Situation – take five…

hackers gaining access into the network is not hard. Assume they are in…appear legitimate. You will need a…

…sophisticated understanding – “the kill chain”

1. Discovery
2. Enumeration
3. Compromise
4. Exploitation
In Cyber Security…Situational Awareness – What is It?

State of Compliance.............or Common Operation Picture (COP)

- Patching: complete, speed?
- Asset Management – do I know what & where my key assets are?
- Provisioning, Access Control and Authentication
- Are we meeting standards?
- Is the enemy in my network
- Disposition of friendly cyber assets
- Enemy able to impact my ability to operate sensors, weapons?
- Intel on the enemy’s weakness – how can I attack the enemy?
We Should Ask Ourselves…

How do we achieve Both?
... to Help We Proposed Something Called ...

THE SECURITY STACK
A Model for Understanding The Cybersecurity We Need

1. Assured System and Content
   - Local and Wide Area Network, Data, Privacy

2. Overlay of Integrated Security
   - Prevent — Detect — Respond

3. Intelligence
   - Situational Awareness (Event Correlation)

4. National Cyber Response
   - National Level Threat Alerts
Thinking First…Our Way to the Right Solutions

... to Help We Proposed Something Called ...

- Starts with Layer 1
- Builds up from bottom
- It is not just Layer 2
- Arrows = Integration
- Layer 3 = Intelligence
- Must have Layer 4
- Sophistication equal to the task
- It is an organized approach to understand the problem and structure the right solution
Layer Three = Situational Awareness

What is needed to improve...

- MSSP services – why is this necessary
- The Security Information and Event Management (SIEM) – state of the technology
- Focus your efforts on what is essential (critical)
- Catch it in the “kill chain”…and on the way out
- It is a “big data” problem
- GRC
Thinking First... Our Way to the Right Solutions

Conceptual Operational View

Continuous Monitoring

<table>
<thead>
<tr>
<th>Security Category</th>
<th>Category Score</th>
<th>Target Category Score</th>
<th>Risk Rating by Category</th>
<th>Category Weighting</th>
<th>Security Score and Risk Rating</th>
<th>Agreed Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Management</td>
<td>71</td>
<td>75</td>
<td>High</td>
<td>4</td>
<td>67 High</td>
<td>79 High</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>84</td>
<td>75</td>
<td>Medium</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance Management</td>
<td>78</td>
<td>60</td>
<td>High</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Management</td>
<td>20</td>
<td>100</td>
<td>Extreme</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Management</td>
<td>40</td>
<td>100</td>
<td>Extreme</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Situational Awareness / Enterprise Security Dashboard

Predict Prevent
- Harden
- Patch
- AV
- Apply Signatures

Detect & Remediate
- CSC defined elements of compromise
- Incident
- Problem
- Change
- Knowledge

Clients

CSC’s Global Threat Intelligence

CAM and LIRM Programs

Help Desk

Cybersecurity

CSC Services

RSA
Alignment with the Security Stack

Continuous Monitoring

<table>
<thead>
<tr>
<th>Security Category</th>
<th>Category Score</th>
<th>Target Category Score</th>
<th>Risk Rating by Category</th>
<th>Category Weighting</th>
<th>Security Score and Risk Rating</th>
<th>Agreed Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Management</td>
<td>71</td>
<td>75</td>
<td>High</td>
<td>4</td>
<td>67 High</td>
<td>79 High</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>64</td>
<td>75</td>
<td>Medium</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance Management</td>
<td>78</td>
<td>60</td>
<td>High</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Management</td>
<td>20</td>
<td>100</td>
<td>Extreme</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Management</td>
<td>40</td>
<td>100</td>
<td>Extreme</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Level 3

Level 4

Level 1 & 2

SOC Services

Help Desk

Level 1

Problem

Change

Knowledge

Cybersecurity

CAM and LIRM Programs

Situational Awareness / Enterprise Security Dashboard

Level 3

Level 3

Level 3

Level 3

Level 1
Thinking First…Our Way to the Right Solutions

Summary & Availability:
Provides Comprehensive Real-time Cyber Situational Awareness

Threat Status

Vulnerability Status

Compliance Status

Incident Status

Risk Status

“See Less, Understand More...”
At A Glance

- **Real-time data:** Enterprise dashboard integrates data from existing security controls into one easy-to-understand dashboard view

- **Highly customizable:** Allows you to customize your dashboard for specific job titles and roles
  - Executive Management, CISO, SOC Analysts, Auditors, etc.

- **Drill-down:** Start with a bird's eye view of your data, and drill down to the smallest of details

- **Technology Agnostic:**
  - SIEM (RSA, Symantec, Arcsight etc)
  - Supports a variety of other security controls

- **Perfect for Traditional & Cloud IT:** Works with traditional and CSC Trusted Cloud IT infrastructure

- **Non Intrusive** No infrastructure changes needed
Captures “controls based evidence”, security information, events, metric across security domains providing a holistic view of security and risk posture.

- **Security Posture**
- **Compliance Management**
- **Vulnerability Management**
- **Threat Management**
- **Incident Management**
- **Change Management**

- System hardening. Compliance to Regulations & Policy
- Status of Security Patching Wintel, Desktop, Unix
- Status of Anti Virus, NIPS, Email & URL Content Filtering

Ensure Change Management requests adhere to Policy.
...start by making sense of the complexity...
THANK YOU

DEAN WEBER
Chief Technology Officer
CSC Cybersecurity
dweber6@csc.com