Building a Security Dashboard

Joel M Snyder
jms@opus1.com
Senior Partner
Opus One
Agenda

• What’s a Dashboard?

• How do I build one (part 1)?

• <parts 2 through n> don’t fit in an hour
A Security Dashboard Provides...

• “At a Glance” view of your security posture
“Security Posture?”
What’s that?

• Since

Security is Risk Avoidance, Joel’s Definition is:

*Security Posture*: The Degree to Which You Are Exposed to Risk
Risk Mitigators Reduce Risk
For Example:

<table>
<thead>
<tr>
<th>Before</th>
<th>Mitigator</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lots of viruses</td>
<td>Anti-virus</td>
<td>A few viruses</td>
</tr>
<tr>
<td>Lots of spam</td>
<td>Anti-spam</td>
<td>A few spam</td>
</tr>
<tr>
<td>Lots of attacks</td>
<td>Intrusion Prevention</td>
<td>A few attacks</td>
</tr>
<tr>
<td>Lots of inappropriate traffic</td>
<td>Content filtering</td>
<td>A little inappropriate traffic</td>
</tr>
<tr>
<td>Lots of leaked data</td>
<td>Data Leak Protection</td>
<td>A little leaked data</td>
</tr>
<tr>
<td>Lots of port scans</td>
<td>Firewall</td>
<td>A few port scans</td>
</tr>
</tbody>
</table>
Anomaly Detectors can Detect Risk

+1 standard deviation

Secondary signs of increase in risk are also visible in the form of anomalous activity
Step 1 of
Building A Dashboard

• Identify Sources of Risk Information
  • Risk mitigation technologies
  • Anomaly detection technologies
  • Traffic flow and information
## Example: Opus One

<table>
<thead>
<tr>
<th>Source of Information</th>
<th>Type of Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Traffic Log</td>
<td>Traffic in/out of the network; prohibited inbound/outbound attempts</td>
</tr>
<tr>
<td>Mail Security Gateway</td>
<td>Level of inbound email traffic; number of viruses and spam blocked</td>
</tr>
<tr>
<td>IDS/IPS</td>
<td>Alerts on suspicious traffic; alerts on blocked traffic</td>
</tr>
<tr>
<td>Network Monitoring</td>
<td>Systems up/down; ping latency; link/disk/memory/CPU usage</td>
</tr>
<tr>
<td>Bandwidth Graphing</td>
<td>Traffic levels at network port granularity</td>
</tr>
<tr>
<td>Vulnerability Analyzer</td>
<td>System vulnerability detection; deltas in vulnerabilities; changes in open ports</td>
</tr>
<tr>
<td>Log Collector</td>
<td>Information from SYSLOG, Windows Event Log, SNMP</td>
</tr>
<tr>
<td>Tripwire</td>
<td>Changes in system security or sensitive files</td>
</tr>
</tbody>
</table>
How Do We Measure Risk Exposure?

Identify assets and define their value
Identify threats to assets

Calculate
\[ SLE = (EF \times Value) + Downtime \]

Calculate
\[ ALE_{\text{before}} = ARO_{\text{before}} \times SLE_{\text{before}} \]

Figure out a solution that mitigates risk

Change EF, ALE, and ARO

Calculate
\[ ALE_{\text{after}} = ARO_{\text{after}} \times SLE_{\text{after}} \]
OK, Better Question: What Do Our Data Tell Us?

- Mitigators can’t tell you when they’re broken
  - But you may be able to see it
- Anomaly detectors can’t tell you when something is broken
  - But you may be able to see it
For Example, Mail Security Gateway

<table>
<thead>
<tr>
<th>Virus Type</th>
<th>Incoming Messages</th>
<th>Outgoing Messages</th>
<th>Total Infected Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mal/Cryp:Box A</td>
<td>101</td>
<td></td>
<td>101</td>
</tr>
<tr>
<td>W32/MyDoom-O</td>
<td>35</td>
<td></td>
<td>35</td>
</tr>
<tr>
<td>Mal/7ipMal-R</td>
<td>33</td>
<td></td>
<td>33</td>
</tr>
<tr>
<td>W32/Netsky-P</td>
<td>15</td>
<td></td>
<td>15</td>
</tr>
<tr>
<td>Mal/Iframe-E</td>
<td>7</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>Troj/Invc-Zip</td>
<td>6</td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>Mal/EncPc-FS</td>
<td>3</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Troj/Inject-EQ</td>
<td>3</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Troj/Inject-FA</td>
<td>3</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Mal/OddZip-A</td>
<td>2</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

What can you see in this information that helps you to evaluate security posture and risk?
This Turns Into...

Email Virus Summary - 28 Feb 2009 00:00 to 03 Mar 2009 14:06

Outbound
Rate: 0, 0, 0
Total: 0

Inbound
Rate: 2, 2, 2
Total: 187

Mal/CryptBox- A (101)
W32/MyDoom- 0 (35)
Mal/ZipMal- B (33)
W32/Netsky- P (15)

1 hr, 8 hr, 100 hr
Or Possibly

Email Virus Summary - 28 Feb 2009 00:00 to 03 Mar 2009 15:21

Outbound
Rate: 10, 0, 0
Total: 10

Inbound
Rate: 2, 2, 2
Total: 187

Eicar (10)

Mal/CryptBox-A (101)
W32/MyDoom-O (35)
Mal/ZipMal-B (33)
Example 2: Network Status
How About: “Who is Slow?”

Remember: “who is down” is not security dashboard—you’ll get alerts for that stuff. We want additional insight on un-alertable data here.
Too Generic: “Who is Unusually Fast/Slow?”

Better... but would be good to color code based on how far off of normal behavior this is. Even better ... don’t fixate on “ping” but extend response time to applications.
Step 2 of Building a Dashboard

2. Reduce output of risk mitigation tools to minimum needed to determine security posture!

If you want the full boat, you can always click-through to the original data or a more detailed display.
Incorporating Anomaly Detection Requires Baselining

Quick: is there something wrong here or not?
Without Baselining, You’ll Never Know

Looks like we kick off backups on Tuesday at midnight for this system.
# Examples of Baseline Deviation

<table>
<thead>
<tr>
<th>Source of Information</th>
<th>Deviation To Look For</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Traffic Log</td>
<td>Traffic high/low; outbound “deny” high</td>
</tr>
<tr>
<td>Network Monitoring</td>
<td>Application “slower” than normal</td>
</tr>
<tr>
<td>Vulnerability Analyzer</td>
<td>Delta in open ports/responding services</td>
</tr>
<tr>
<td>Log Collector</td>
<td>SYSLOG/Windows Log/SNMP Trap above normal levels for each system</td>
</tr>
<tr>
<td>Tripwire</td>
<td>Tripwire is all about deviations!</td>
</tr>
</tbody>
</table>
Step 3 of Building a Dashboard

3. Determine sliding baseline for security metrics and report when baseline is exceeded

You will also want to have pure bandwidth graphs on your dashboard, but you don’t have room for too many.
Next Steps

4. Identify most critical 12 to 16 “panes” of data giving insight into security posture

5. Bring together into graphical format

6. Reconcile with alerting

7. Get promotion from drooling boss
Thanks!

Joel M Snyder
jms@opus1.com
Senior Partner
Opus One