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…

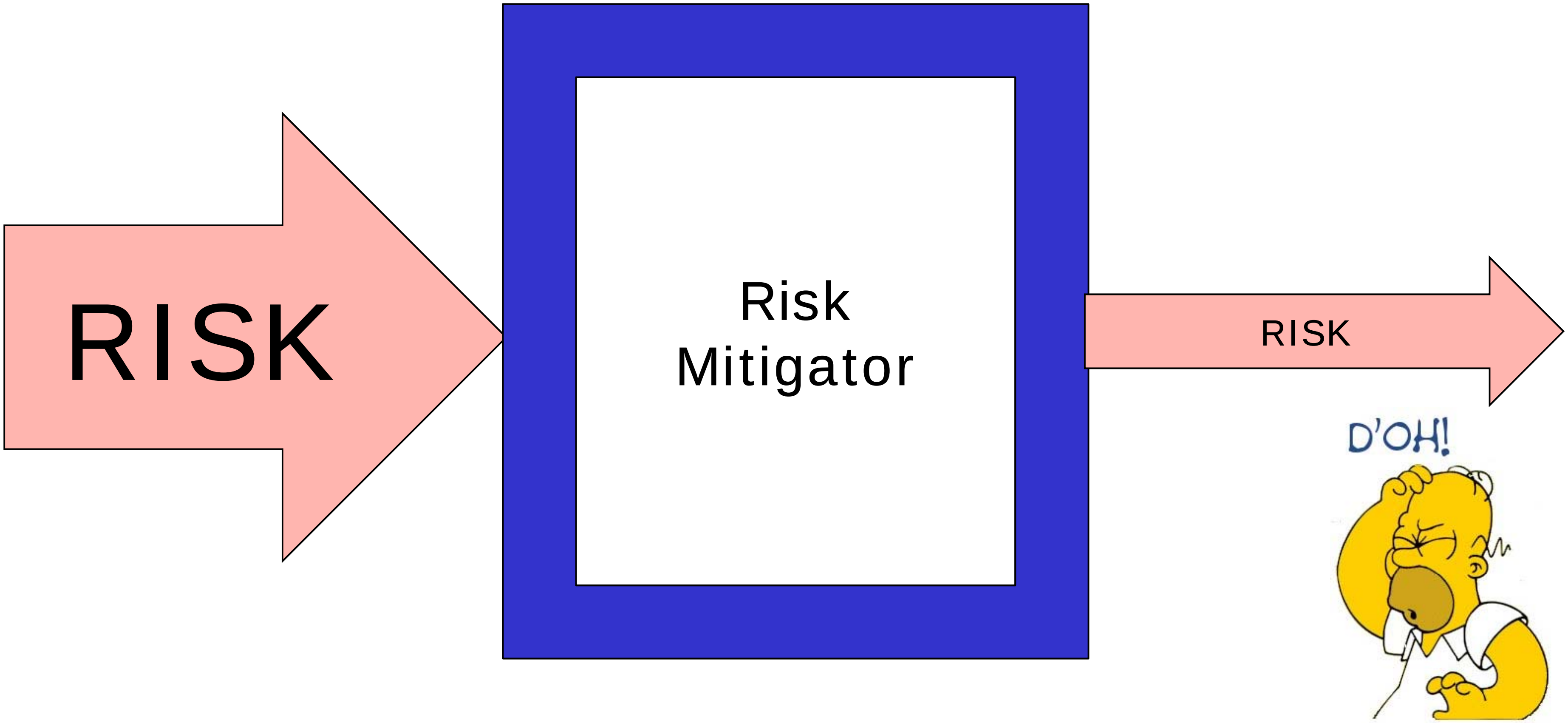
- “At a Glance” view of your security posture

"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



RISK

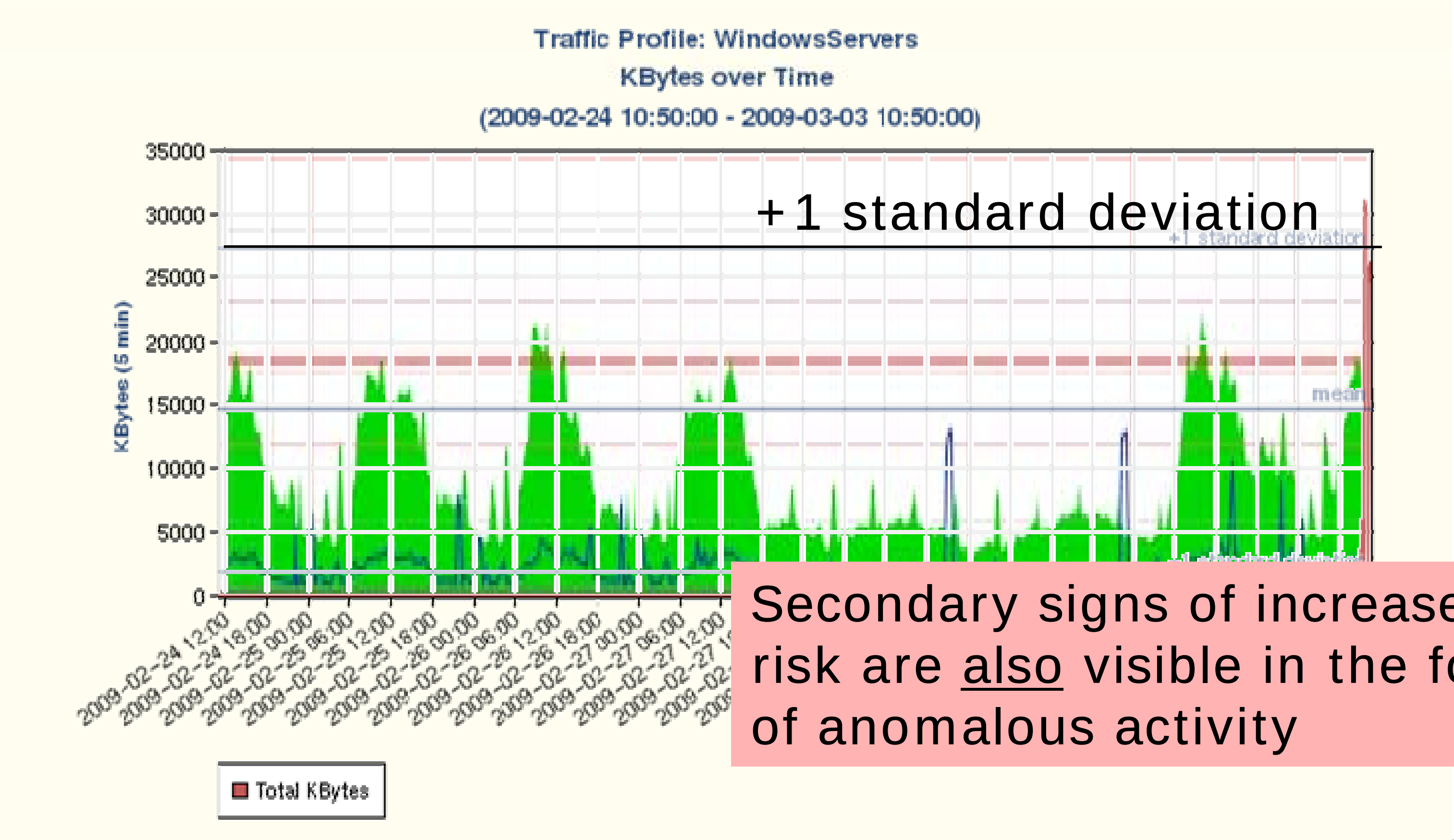
Risk Mitigator

RISK

For Example:

Before	Mitigator	After
Lots of viruses	Anti-virus	A few viruses
Lots of spam	Anti-spam	A few spam
Lots of attacks	Intrusion Prevention	A few attacks
Lots of inappropriate traffic	Content filtering	A little inappropriate traffic
Lots of leaked data	Data Leak Protection	A little leaked data
Lots of port scans	Firewall	A few port scans

Anomaly Detectors can Detect Risk



+1 standard deviation

Secondary signs of increase in risk are <u>also</u> visible in the form of anomalous activity

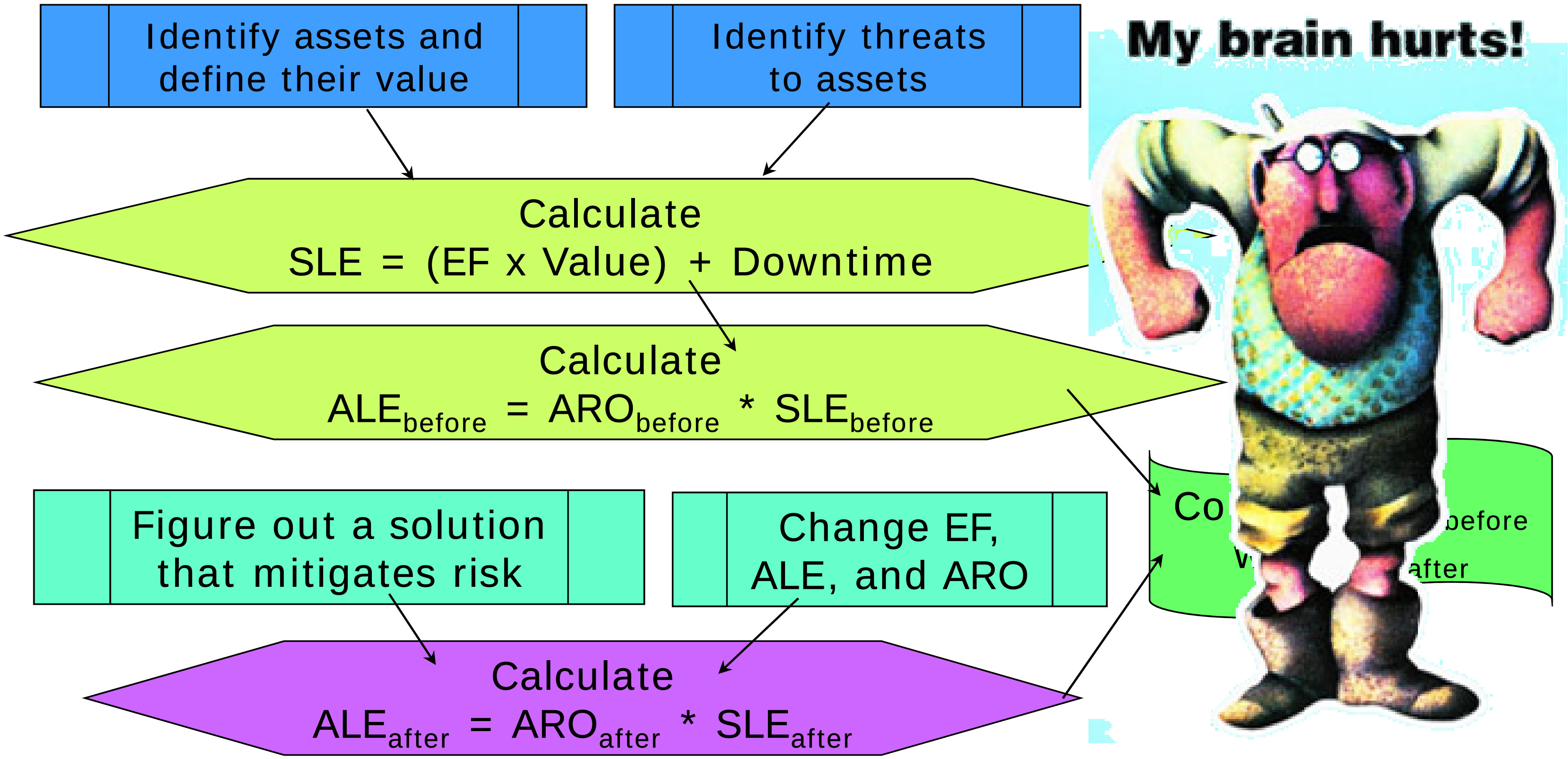
Step 1 of
Building A Dashboard

- Identify Sources of Risk Information
  - Risk mitigation technologies
  - Anomaly detection technologies
  - Traffic flow and information

Example: Opus One

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

How Do We Measure Risk Exposure?



Identify assets and define their value

Identify threats to assets

Calculate SLE = (EF x Value) + Downtime

Calculate $ALE_{before} = ARO_{before} * SLE_{before}$

Figure out a solution that mitigates risk

Change EF, ALE, and ARO

Calculate $ALE_{after} = ARO_{after} * SLE_{after}$

Co

before

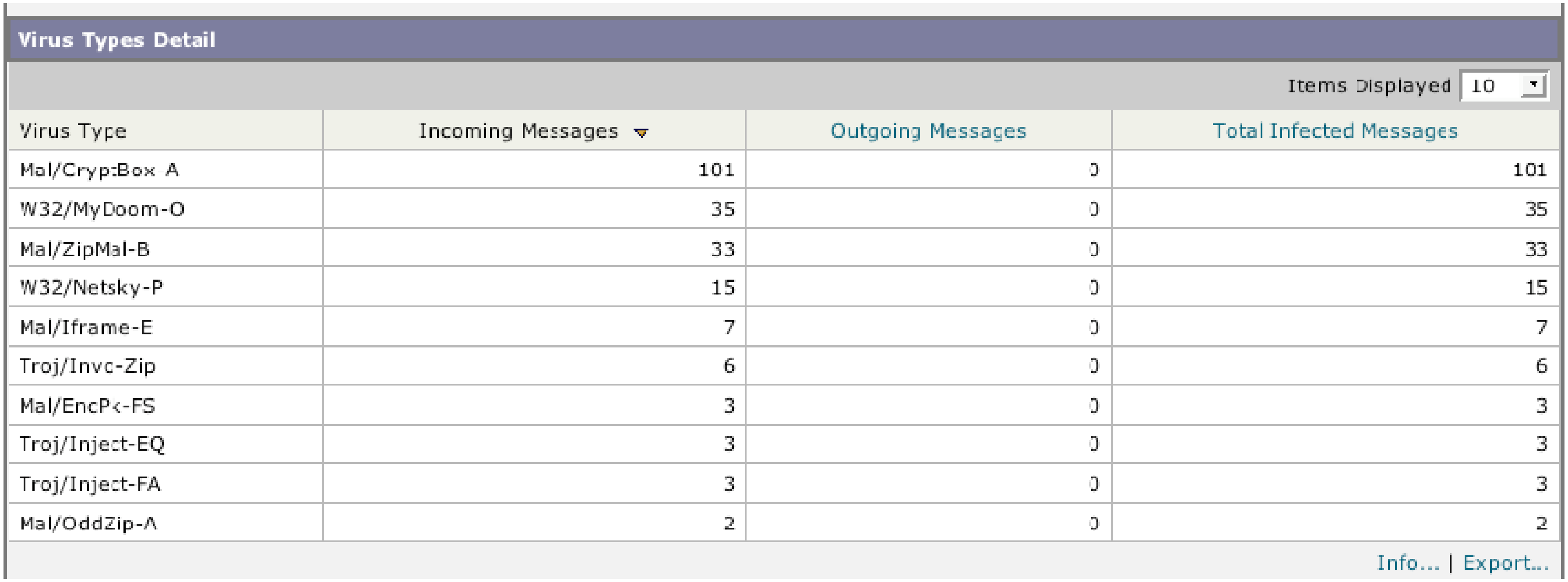
W

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



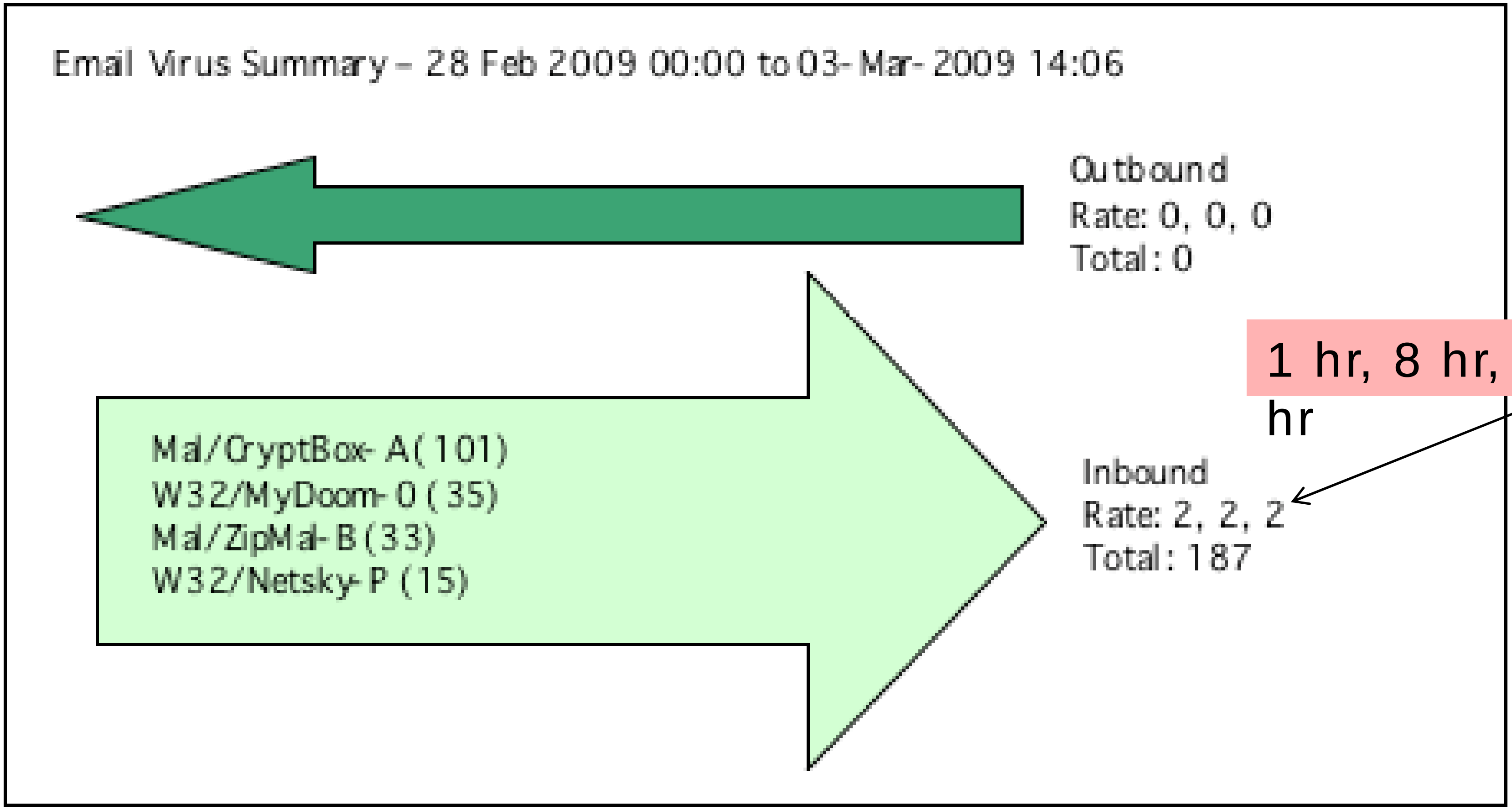
Virus Types Detail

Items Displayed 10

Virus Type	Incoming Messages ▼	Outgoing Messages	Total Infected Messages
Mal/CrypBox-A	101	0	101
W32/MyDoom-O	35	0	35
Mal/ZipMal-B	33	0	33
W32/Netsky-P	15	0	15
Mal/Iframe-E	7	0	7
Troj/Invo-Zip	6	0	6
Mal/EncPk-FS	3	0	3
Troj/Inject-EQ	3	0	3
Troj/Inject-FA	3	0	3
Mal/OddZip-A	2	0	2

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

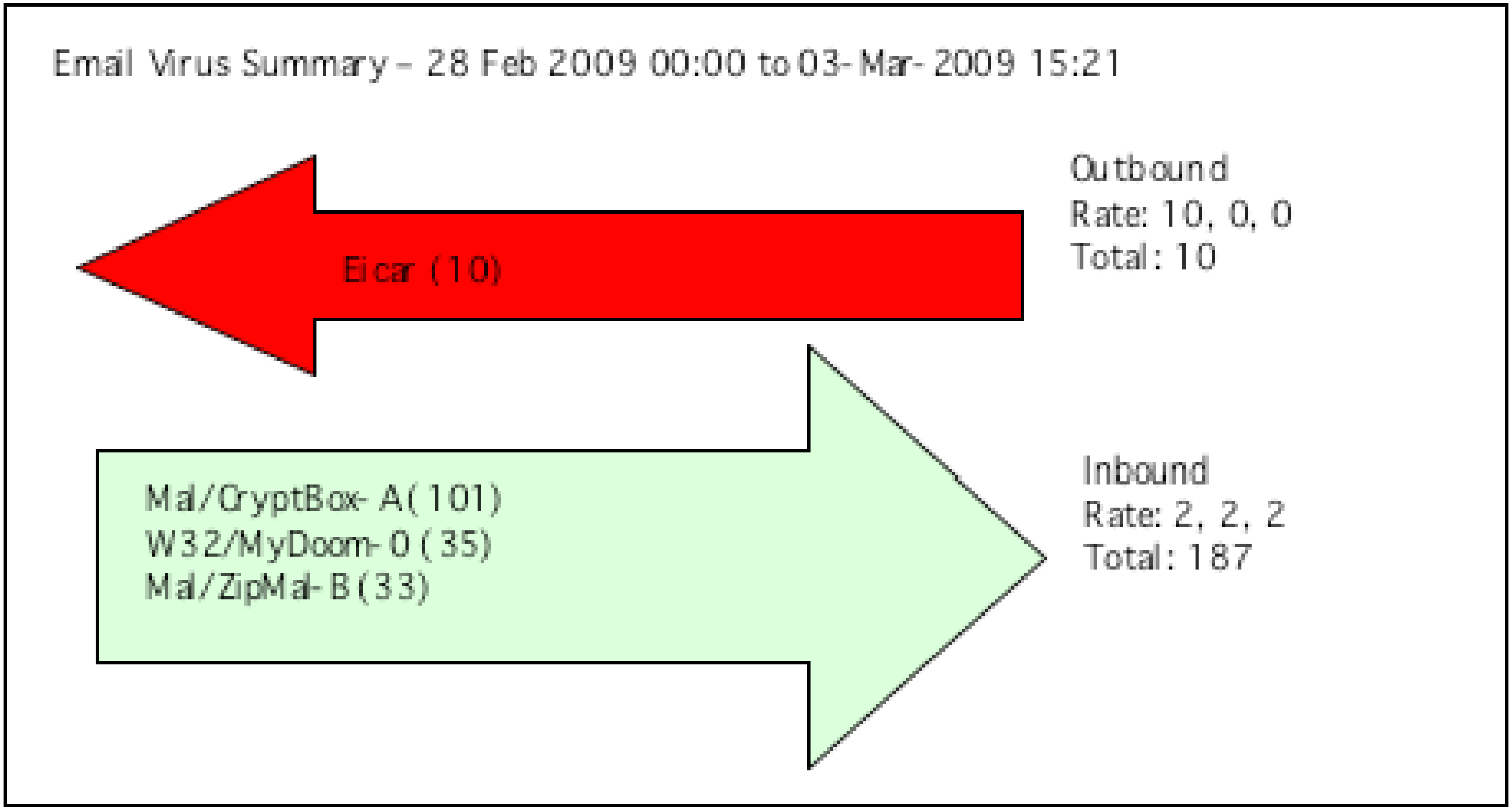
Outbound
Rate: 0, 0, 0
Total: 0

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

Inbound
Rate: 2, 2, 2
Total: 187

1 hr, 8 hr, 100 hr

Or Possibly



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

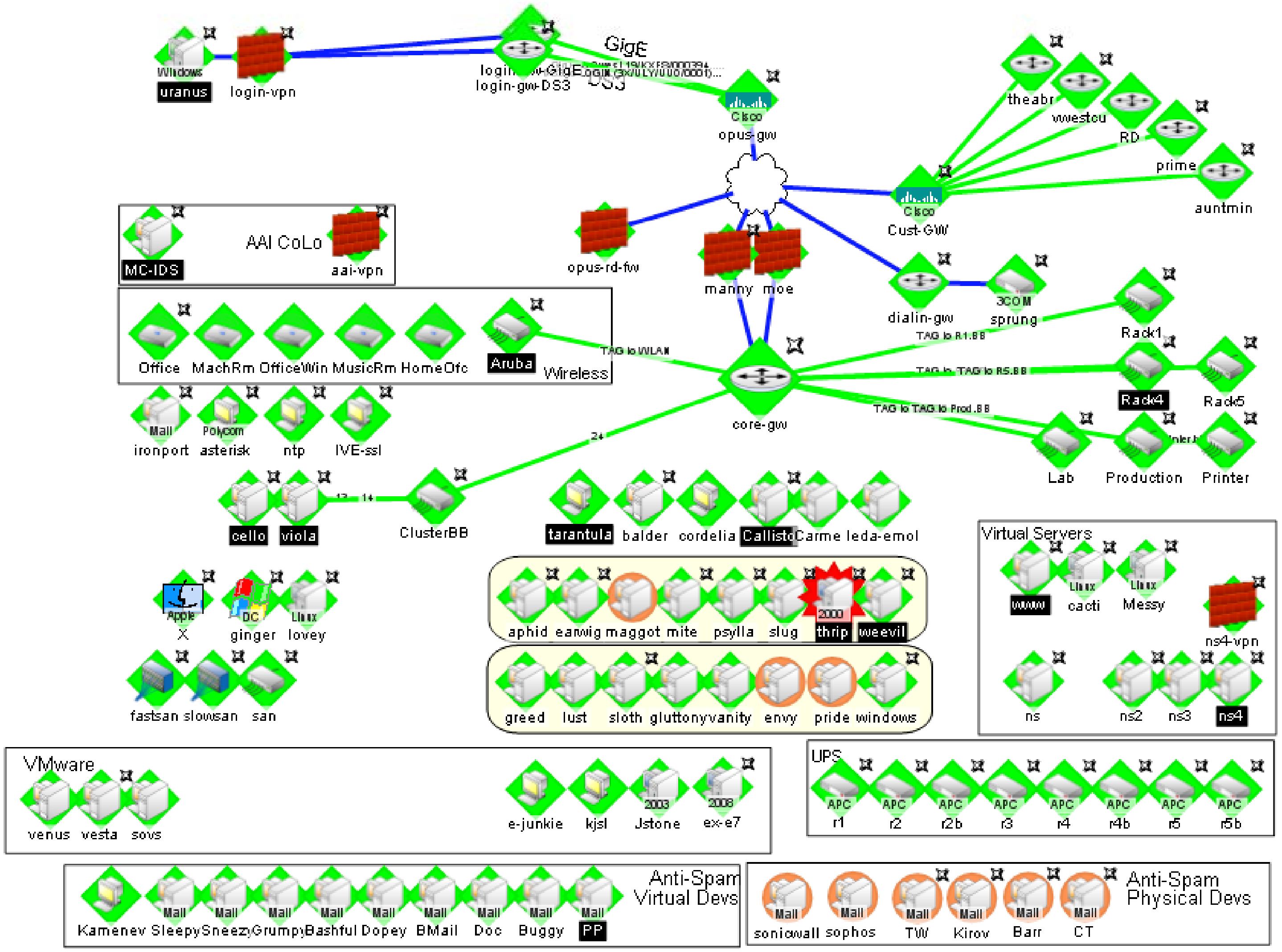
Eicar (10)

Outbound
Rate: 10, 0, 0
Total: 10

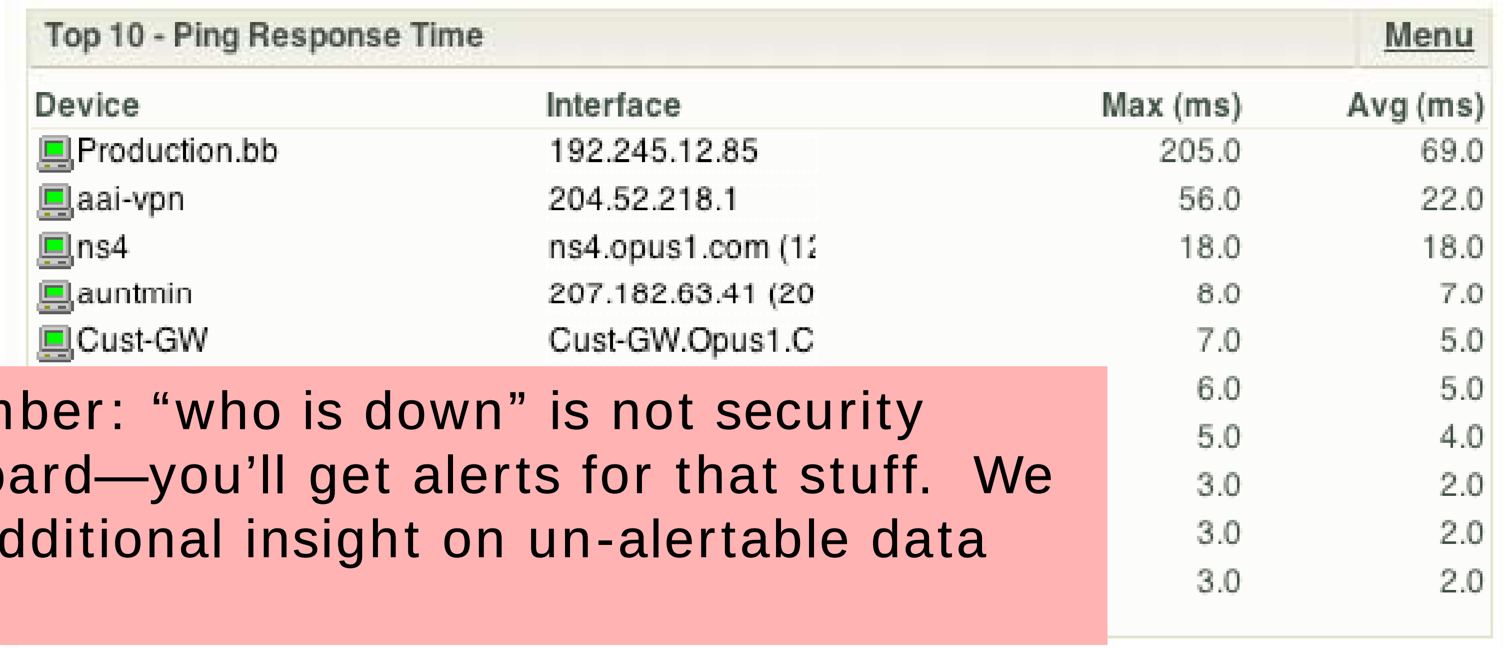
Mal/CryptBox-A (101)
W32/MyDoom-O (35)
Mal/ZipMal-B (33)

Inbound
Rate: 2, 2, 2
Total: 187

Example 2: Network Status



How About: “Who is Slow?”

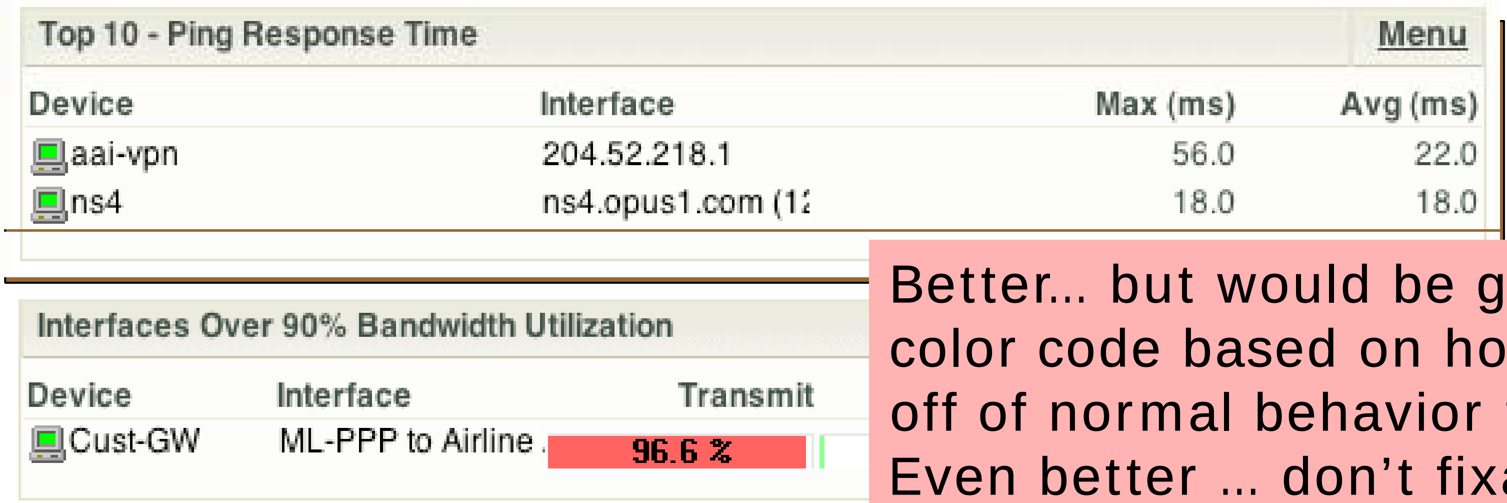


Top 10 - Ping Response Time Menu

Device	Interface	Max (ms)	Avg (ms)
Production.bb	192.245.12.85	205.0	69.0
aai-vpn	204.52.218.1	56.0	22.0
ns4	ns4.opus1.com (1	18.0	18.0
auntmin	207.182.63.41 (20	8.0	7.0
Cust-GW	Cust-GW.Opus1.C	7.0	5.0
		6.0	5.0
		5.0	4.0
		3.0	2.0
		3.0	2.0
		3.0	2.0

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?”



Top 10 - Ping Response Time | Menu

Device	Interface	Max (ms)	Avg (ms)
aai-vpn	204.52.218.1	56.0	22.0
ns4	ns4.opus1.com (1:	18.0	18.0

Interfaces Over 90% Bandwidth Utilization

Device	Interface	Transmit
Cust-GW	ML-PPP to Airline .	96.6 %

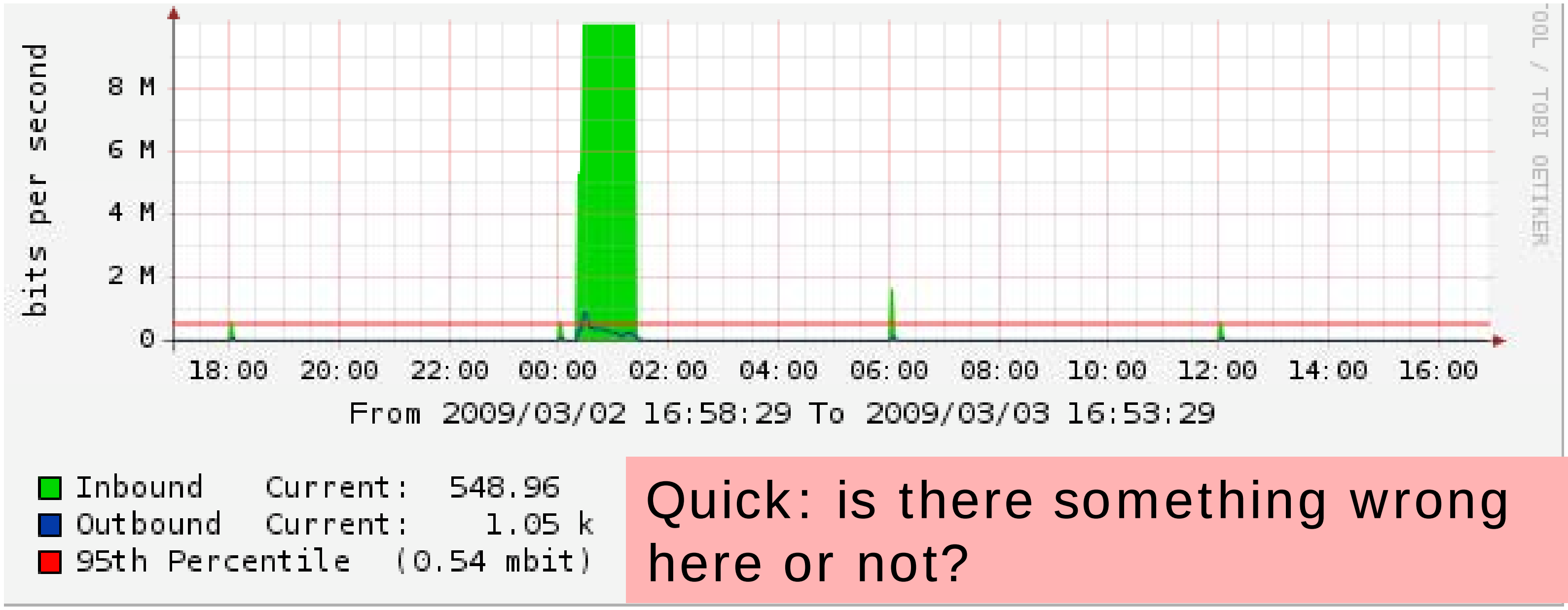
Better… but would be good to color code based on how far off of normal behavior this is. Even better … don’t fixate on “ping” but extend response time to applications

Step 2 of
Building a Dashboard

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

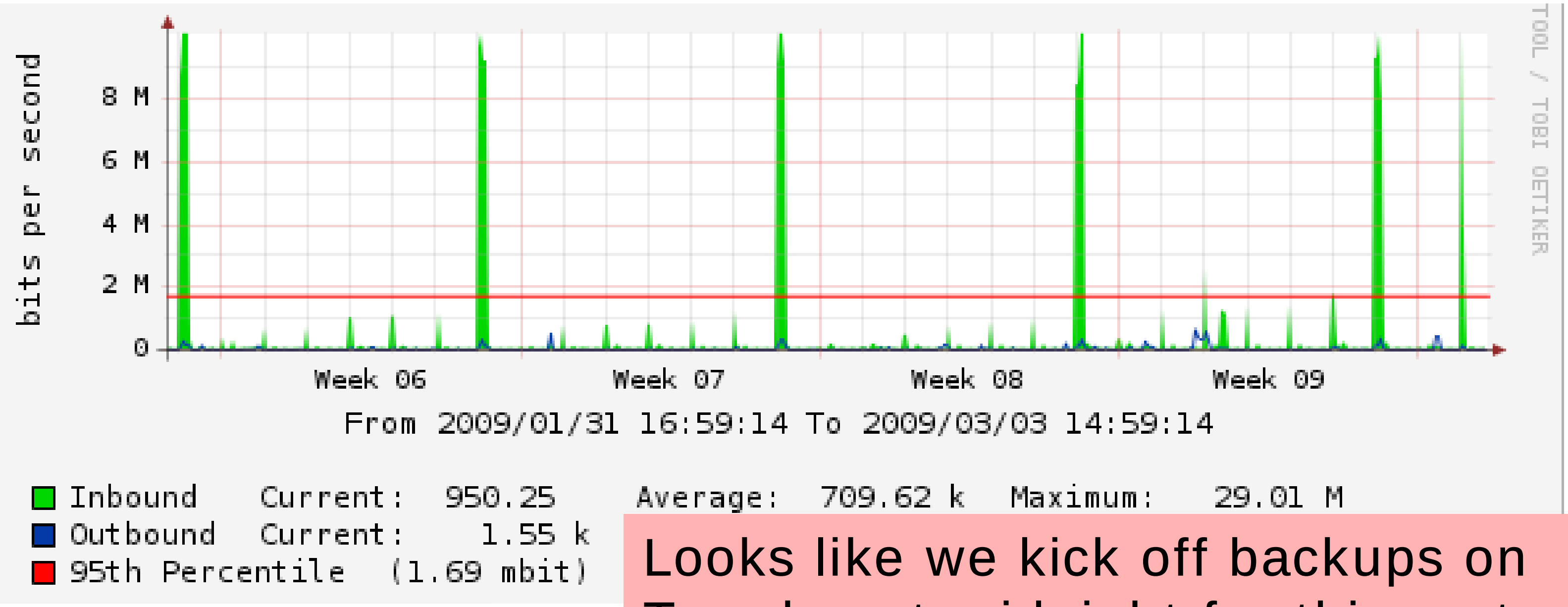
If you want the full boat, you can always click-through to the original data or a more detailed display

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

Source of Information	Deviation To Look For
Firewall Traffic Log	Traffic high/low; outbound "deny" high
Network Monitoring	Application "slower" than normal
Vulnerability Analyzer	Delta in open ports/responding services
Log Collector	SYSLOG/Windows Log/SNMP Trap above normal levels for each system
Tripwire	Tripwire is all about deviations!

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