Is Your Network a Sitting Duck?
3 Secrets to Securing Your Information Systems

Presenter: Matt Harkrider

Founder, Alert Logic
Who We Are: Corporate Fact Sheet

- Founded: 2002
- HQ: Houston, TX
- Privately held
- Customers: 200 +
- Service renewal rate: 99%
- Focus: Network Intrusion Defense
- Key differentiator:
  - On-Demand delivery model

Sample Customers:

- bhpbilliton
- BMW
- Eni Petroleum
- Tauber Oil Company
- LEGO
- HISD Connect
- Acergy
- ANDREWS KURTH, LLP
- COLUMBIA COLLEGE
- Bracewell & Giuliani LLP
- Kanaly Trust Company
- smart:financial
- NexT Financial Group
- Franklin Bank
- Pinnacle Financial Strategies
False Sense of Security

According to the recent FBI/CSI survey:

- 97% utilize firewalls
- 96% have Anti-Virus

Breaches continue...
- 56% reported breach
- Avg loss = $200,000
Third Layer of Security is Required

Gartner’s Top Predictions for IT Organizations and Users, 2007 and Beyond

- "By the end of 2007, we believe that three out of four organizations will be infected with financially motivated, targeted malware that has evaded their traditional perimeter and host defenses and remains installed and undetected on their endpoints…"

- “…antivirus and firewalls are insufficient for comprehensive malicious-code detection and prevention. Legacy antivirus mechanisms must be supplemented with more-advanced styles of intrusion prevention in network- and host-based security…."

- “…addressing targeted threats should not require that organizations purchase dozens of new security point solutions. Rather, security platforms should evolve to deliver more types of security protection for little or no additional cost.”
The 3 Secrets
3 Secrets

2. Proactive vulnerability scanning
3. Network threat monitoring
4. Don’t “do it yourself”
Vulnerabilities
Dangerous Trends

• Time to vulnerability window has collapsed
• Attack vectors change faster than any organization can respond
• Too much emphasis placed on perimeter security
Vulnerability to threat timeline

Exploit code released

Widespread exploitation (worms, targeted attacks)

Vulnerability is discovered

Advisory Release

Vulnerability to threat window is rapidly collapsing
Historical Evidence

- **Nimda**
  - MS00-078
  - Oct 17 2000
  - Sep 18 2001
  - 365 days

- **SQL Slammer**
  - MS02-039
  - Jul 24 2002
  - Aug 11 2003
  - 26 days
  - Jan 25 2003
  - 185 days

- **MS Blaster**
  - MS03-026
  - Jul 16 2003
  - Aug 11 2003
  - 26 days

- **Sasser**
  - MS04-011
  - Apr 22 2004
  - May 2 2004
  - 20 days

- **ZOTOB**
  - MS05-039
  - Aug 9, 2005
  - Aug 14 2005
  - 5 days

**NOTE:**
- **MS04-011**
  - Apr 22 2004
  - May 2 2004
  - 20 days

**ALERTLOGIC**

Network Protection On Demand
New Vectors Emerge Quickly

Malware spreads through new vectors with ease

Security does not react fast enough to sudden shifts in direction
Network Threat Monitoring
Attacker Trends

• Attackers are better at “flying under the radar”
  – Fewer flashy, public attacks - more stealth intrusions
  – Botnets emerging as a valuable commodity
  – Threats are free to propagate throughout the network
  – Corporate security staffs not properly equipped to keep up with latest threats
Network Dangers

- Firewall Penetrating Worms
- Unauthorized Access
- Threats From Roaming Laptops
- Botnets

Diagram:
- Web Server
- Workstation
- Firewall
- Switch
- Financial App Server
- Customer DB Server
- Email or File Server
- Laptop
- Internet

Network Protection On Demand

ALERTLOGIC
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>command.list</td>
<td>List of all the available commands</td>
</tr>
<tr>
<td>bot.dns</td>
<td>Resolves an IP/hostname</td>
</tr>
<tr>
<td>bot.execute</td>
<td>Runs an .exe file on a remote computer</td>
</tr>
<tr>
<td>bot.open</td>
<td>Opens a file on a remote computer</td>
</tr>
<tr>
<td>bot.command</td>
<td>Runs a command with system()</td>
</tr>
<tr>
<td>irc.server</td>
<td>Connects to an IRC server</td>
</tr>
<tr>
<td>irc.join</td>
<td>Enters a specific channel</td>
</tr>
<tr>
<td>irc.privmsg</td>
<td>Sends a private message to a user</td>
</tr>
<tr>
<td>http.execute</td>
<td>Downloads and executes a file through HTTP</td>
</tr>
<tr>
<td>ftp.execute</td>
<td>Downloads and executes a file through FTP</td>
</tr>
<tr>
<td>ddos.udpflood</td>
<td>Starts a UDP flood</td>
</tr>
<tr>
<td>ddos.synflood</td>
<td>Starts a Syn flood</td>
</tr>
<tr>
<td>ddos.phaticmp</td>
<td>Starts a PHATicmp flood</td>
</tr>
<tr>
<td>redirect.http</td>
<td>Starts a HTTP proxy</td>
</tr>
<tr>
<td>redirect.socks</td>
<td>Starts a SOCKS4 proxy</td>
</tr>
<tr>
<td>pctrl.list</td>
<td>List of processes</td>
</tr>
<tr>
<td>pctrl.kill</td>
<td>Kills the process</td>
</tr>
</tbody>
</table>

**What Can You Do With Bots?**
Threats Free to Propagate

• Lack of visibility into network traffic
• No control mechanisms to stop threats once they begin to spread
• Insider threats attempting unauthorized access
Losing the Arms Race

• Most businesses ill equipped to effectively fight the bad guys

• Network security solutions complicated and difficult to deploy – “too many moving parts”
Why You Shouldn’t “Do It Yourself”
How We Compare

“Do it Yourself” Appliance/Software
- Hardware cost
- Software cost
- Maintenance costs
- Care and feeding
- Lengthy deployment
- Labor intensive
- Requires in-house expertise

Outsource To MSSP
- Hardware cost
- Software cost
- No visibility
- Loss of control

Network Security Options Spectrum

Alert Logic On Demand Protection
- Rapid deployment
- Zero maintenance
- No software or hardware costs
- Complete control and visibility
- Superior accuracy
Layered “On-Demand” (SaaS) Model

Optional SOC Services

Moving Parts Are Hosted in Our Datacenter

Network Appliance(s)
Three Products in One

Intrusion Protection
• Leverages 8,000+ signatures
• Passive monitoring with optional blocking, containment, & quarantine defensive actions
• SSL embedded threat detection
• Incident resolution management

Vulnerability Management
• PCI certified scanning (available in Q1 ’07)
• Automated scanning with 12,000+ vulnerabilities
• Network discovery and asset weighting
• On-Demand external and internal scanning (external available Q1 ’07)
• Exposure remediation resolution management

Compliance Reporting
• Compliance posture security Incident identification
• Compliance posture vulnerability identification
• Pre-built PCI, SOX, GLBA, and HIPAA reporting
Threat Manager in Action
Search Incidents
View All Incidents
Search Events
View All Events

Configure Incident Monitor
Configure Event Monitor
Configure Alerts

Did you Know?
You can be automatically alerted of new threats. Configure your event alert rules to enable this feature.

Latest Incidents
Top Incidents
By Threat
By Status
By Classification
Worms Spreading

<table>
<thead>
<tr>
<th>ID</th>
<th>Summary</th>
<th>Date</th>
<th>Threat</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>27366</td>
<td>Webserver responded to a cmd.exe attack</td>
<td>Today 05:02:49</td>
<td>73</td>
<td>68</td>
</tr>
<tr>
<td>18002</td>
<td>Nikto vulnerability scan</td>
<td>Mar 19 2007 11:42:52</td>
<td>74</td>
<td>2</td>
</tr>
<tr>
<td>34107</td>
<td>PnP QueryResConfList exploit attempt from 10.0.2.2</td>
<td>Mar 13 2007 13:40:20</td>
<td>66</td>
<td>74</td>
</tr>
</tbody>
</table>

View All Incidents
Executive Summary

The SOX Executive Summary lists specific of security controls that relate to data collected by Invision Security. For each general category, the specific of controls are listed, with their respective issue counts. If any category has issues present, the number of issues will be listed and clicking on that category title will provide further information about the issues affecting it.

Access

Unauthorized Access to Financial Systems

Weak Passwords

Default User Accounts

Configuration Management

Latest Patches Not Installed

Incidents
Feature/Benefit Summary

• 3-in-1 Solution
  – Fully integrated solution eliminates the difficult task of correlating data from multiple sources to get a comprehensive picture of the security posture of your network.

• 24x7 Monitoring
  – Alert Logic is always keeping an eye on your network, even when you can’t. This ensures threats are addressed in the timeliest fashion to secure your network before damage can occur, freeing your staff to perform other high-priority tasks.

• Co-Managed w/ Full Visibility
  – Alert Logic’s On-Demand model means that we do it all for you. But you maintain full visibility and control over network security using the same GUI as the Alert Logic 24x7 monitoring team.

• Blocking and Containment
  – We can terminate communication to/from a threatened asset at the firewall and either contain or quarantine at the switch, thereby eliminating threats before they harm your network.

• Extensive compliance reports
  – Comprehensive reporting includes detailed and executive-level reports, providing easy communication of network security posture and helping to satisfy compliance requirements.

• No Maintenance Required
  – Alert Logic manages all upgrades, updates, and maintenance of the application, freeing your staff from this expensive and time-consuming task.

• Simple one-day installation
  – Alert Logic’s On-Demand solution eliminates the implementation burden associated with do-it-yourself solutions. This ensures a successful one-day installation and frees your staff from the expensive and time-consuming task of setting up hardware, loading software, network rollout, QA, and testing.
What should you do?

• Stop thinking of network threats as a nuisance
• Stop focusing exclusively on the perimeter
  – Inside of firewalls networks are wide open today
  – Businesses continuously spend 80% of their budget to fix 20% of their problem
• Automate incident investigation and response
  – Defense today is shrouded in uncertainty and reliant on manual decisions
  – Few businesses have situational awareness that allows them to identify complex threat scenarios
  – Network security has to become automated to be effective
In Summary

• Security issues are much more prevalent but rarely get the appropriate attention
• Perimeter security is limited in it’s ability to prevent Network Threats
• Attackers and their exploits may take multiple vectors to achieve their goals
• Additional layers of defense should reduce burden on you, not be a burden