Agenda

- Four Themes Shaping CyberSecurity
- Existing Means of Dealing With Them
- What is Lacking
- IBM's Vision

- And, of course, the Obligatory Marketing Slide
Four themes shape our world (Well, the IT parts)

Innovative Technology

Extreme Threats

New Approach

New Leadership
Innovative technology changes everything

- 1 trillion connected objects
- Social business
- Cloud and virtualization
- 1 billion mobile workers
- Bring your own IT
Motivations and sophistication are rapidly evolving

- **National Security**
  - Nation-state actors
    - Stuxnet

- **Espionage, Activism**
  - Competitors and Hacktivists
    - Aurora

- **Monetary Gain**
  - Organized crime
    - Zeus

- **Revenge, Curiosity**
  - Insiders and Script-kiddies
    - Code Red
Techniques, tools, and targets are also increasing.

In 2011 there was an 80% increase in phishing attacks, many of which impersonate social networking sites.

In 2011 there was a 19% increase in the number of tools released publicly that can be used to attack mobile devices.

So far in 2012, IBM reports over 4,400 new security vulnerabilities.

Source: IBM X-Force® 2011 Trend and Risk Report
Nobody is immune. There is no end in sight.

2011 Sampling of Security Incidents by Attack Type, Time and Impact

Source: IBM X-Force® Research 2011 Trend and Risk Report
And lest you think it's getting better: the 2012 picture

Source: IBM Xforce 2012 Trend and Risk Report
So, What Do We Do?

Buy More Tools
 Seriously, What Do We Do?

Well, We Buy More Tools

The IBM Sales Guys are going to scream here, but we already have a ton of tools, and what do we get for it?
Your security team sees noise
We (IT People) Think in Terms of Infrastructure

<table>
<thead>
<tr>
<th>Infrastructure</th>
<th>Datacenters</th>
<th>PCs</th>
<th>Laptops</th>
<th>Mobile</th>
<th>Cloud</th>
<th>Non-traditional</th>
</tr>
</thead>
</table>
But That's Not Right:

CyberSecurity challenges are a complex, four dimensional puzzle
So What, Then?
Then: Administration

• Identity management
• Cost control

Now: Insight

• Identify and monitor highest risk users
• Know who has access to sensitive data and systems
• Baseline normal behavior
• Prioritize privileged identities

Monitor Everything
Data

Then: Basic Control

• Simple access controls and encryption

Now: Laser Focus

• Discover and protect high-value data

• Understand who is accessing the data, at what time of day, from where, and in what role

• Baseline normal behavior

Monitor Everything
Applications

Then: **Bolt-on**

- Periodic scanning of Web applications

Now: **Built-in**

- Harden applications with access to sensitive data
- Scan source and real-time
- Baseline normal application behavior and alert

Monitor Everything

Infrastructure

Then: **Thicker Walls**

- Firewalls, manual patching, and antivirus
- Focus on perimeter security

Now: **Smarter Defenses**

- Baseline system and network behavior
- Analyze unknown threats using advanced heuristics
- Expand coverage into cloud and mobile environments

Monitor Everything
Advanced Research

<table>
<thead>
<tr>
<th>Domain</th>
<th>IP Address</th>
<th>File Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>dogpile.com</td>
<td>117.0.178.252</td>
<td>c69d172078b439545dfff28f3d3aacc1</td>
</tr>
<tr>
<td>kewww.com.cn</td>
<td>83.14.12.218</td>
<td>51e65e6c798b03452ef7ae3d03343d8f</td>
</tr>
<tr>
<td>ynnsuue.com</td>
<td>94.23.71.55</td>
<td>6bb6b9ce713a00d3773cfcecece515e02</td>
</tr>
</tbody>
</table>

Monitor Everything

Then: Reaction

• Read about the latest threats from blogs and news

• Match against known signatures and bad actors

Now: Situational Awareness

• Consume real-time intelligence about the latest threats

• Correlate alerts against external behavior and reputation

• Proactively block bad domains, IP address and malware
Monitor Everything
Consume Threat Intelligence
Integrate Across Domains
Better protection against sophisticated attacks

On the Network
- Application Control
- Network Anomaly Detection
- Web Application Protection
- Content and Data Security
- Intrusion Prevention

Across the Enterprise
- Risk Management
- Vulnerability Management
- Network Activity Monitoring
- SIEM
- Log Management

Across the World
- Threat Advisories
- IP Reputation
- Malware Information
- Malicious Websites
- Vulnerability Database

- Misconfigured Firewall
- 0day Exploit
- Malicious PDF
- Phishing Campaign
- Vulnerable Server
- Spammer
- SQL Injection
- Brute Force
- Malicious Insider
- Infected Website
- Botnet Communication
- Malicious Insider

Obligatory Marketing Section

IBM delivers security solutions across a comprehensive framework

Intelligence

Integration

Expertise
IBM's Tools and Services

- IBM Global Technology Services
- IBM Global Business Services
- IBM Software Group

- Managed Security Services – Management & Intelligence
- Q1 Radar – Data Mining and Intelligence
- Tivoli Suite – Identity and Systems Management and Control Tools
- IBM Cloud Security – Federation,
- IBM Mobile Security – Device, Network, Data and Access Security