Defending Against Cyber Attacks :
Defense & Response Strategies

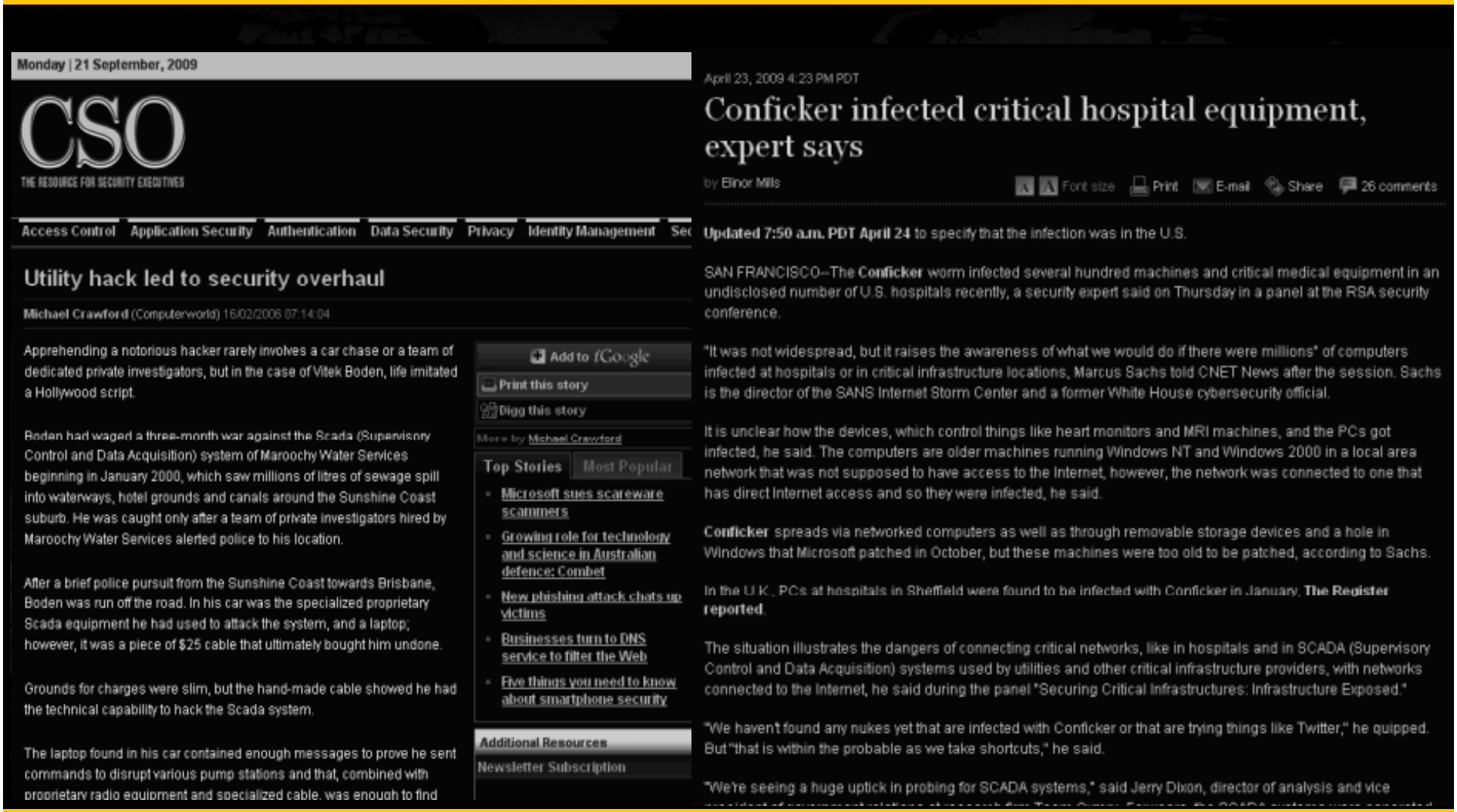
Tan Wei Ming, Senior Manager, Government Relations, APJ

2009 ITU Regional Cybersecurity Forum for Asia-Pacific

24 September 2009, Hyderabad

symantec.

How Likely Are These?



Monday | 21 September, 2009

CSO

THE RESOURCE FOR SECURITY EXECUTIVES

Access Control | Application Security | Authentication | Data Security | Privacy | Identity Management | Sec

Utility hack led to security overhaul

Michael Crawford (Computerworld) 16/02/2006 07:14:04

Apprehending a notorious hacker rarely involves a car chase or a team of dedicated private investigators, but in the case of Vitek Boden, life imitated a Hollywood script.

Boden had waged a three-month war against the Scada (Supervisory Control and Data Acquisition) system of Maroochy Water Services beginning in January 2000, which saw millions of litres of sewage spill into waterways, hotel grounds and canals around the Sunshine Coast suburb. He was caught only after a team of private investigators hired by Maroochy Water Services alerted police to his location.

After a brief police pursuit from the Sunshine Coast towards Brisbane, Boden was run off the road. In his car was the specialized proprietary Scada equipment he had used to attack the system, and a laptop; however, it was a piece of $25 cable that ultimately bought him undone.

Grounds for charges were slim, but the hand-made cable showed he had the technical capability to hack the Scada system.

The laptop found in his car contained enough messages to prove he sent commands to disrupt various pump stations and that, combined with proprietary radio equipment and specialized cable, was enough to find

Add to iGoogle

Print this story

Digg this story

More by Michael Crawford

Top Stories | Most Popular

- Microsoft sues scareware scammers
- Growing role for technology and science in Australian defence: Combet
- New phishing attack chats up victims
- Businesses turn to DNS service to filter the Web
- Five things you need to know about smartphone security

Additional Resources

Newsletter Subscription

April 23, 2009 4:23 PM PDT

Conficker infected critical hospital equipment, expert says

by Elinor Mills

Font size | Print | E-mail | Share | 26 comments

Updated 7:50 a.m. PDT April 24 to specify that the infection was in the U.S.

SAN FRANCISCO--The **Conficker** worm infected several hundred machines and critical medical equipment in an undisclosed number of U.S. hospitals recently, a security expert said on Thursday in a panel at the RSA security conference.

"It was not widespread, but it raises the awareness of what we would do if there were millions" of computers infected at hospitals or in critical infrastructure locations, Marcus Sachs told CNET News after the session. Sachs is the director of the SANS Internet Storm Center and a former White House cybersecurity official.

It is unclear how the devices, which control things like heart monitors and MRI machines, and the PCs got infected, he said. The computers are older machines running Windows NT and Windows 2000 in a local area network that was not supposed to have access to the Internet, however, the network was connected to one that has direct Internet access and so they were infected, he said.

Conficker spreads via networked computers as well as through removable storage devices and a hole in Windows that Microsoft patched in October, but these machines were too old to be patched, according to Sachs.

In the U.K., PCs at hospitals in Sheffield were found to be infected with Conficker in January, **The Register reported**.

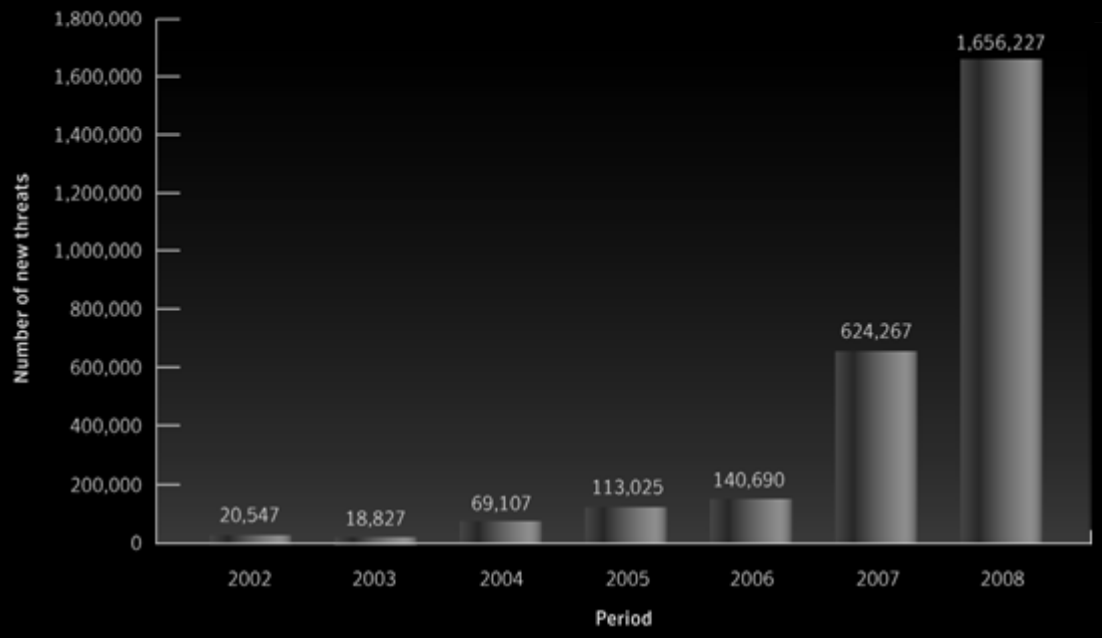
The situation illustrates the dangers of connecting critical networks, like in hospitals and in SCADA (Supervisory Control and Data Acquisition) systems used by utilities and other critical infrastructure providers, with networks connected to the Internet, he said during the panel "Securing Critical Infrastructures: Infrastructure Exposed."

"We haven't found any nukes yet that are infected with Conficker or that are trying things like Twitter," he quipped. But "that is within the probable as we take shortcuts," he said.

"We're seeing a huge uptick in probing for SCADA systems," said Jerry Dixon, director of analysis and vice

Exponential Spike In Malicious Activities

More malicious programs were detected in the last 18 months than in all the previous years combined



Symantec Internet Security Threat Report (Trends for 2008), volume XIV, published April 2009

Cyber Defense – A Mission Impossible?

Disruption of critical infrastructure operations

Large-scale DDoS attacks

Defacing of government websites

Malware outbreaks within government network

Stealthy ex-filtration or unintended loss of confidential data

Effective Cyber Defense & Incident Response Strategy

> 4 important principles

- Understand the threats
- Establish prioritised risk-based framework
- Develop intelligence-in-depth
- Develop strong defense capabilities

1>Understand The Threats

Threat Landscape

The Web is the focal point

- Primary vector for malicious activity
- Target reputable, high-traffic websites

Attackers want YOUR information

- Focus on exploits targeting end-users for financial gain

Increased sophistication of the Underground Economy

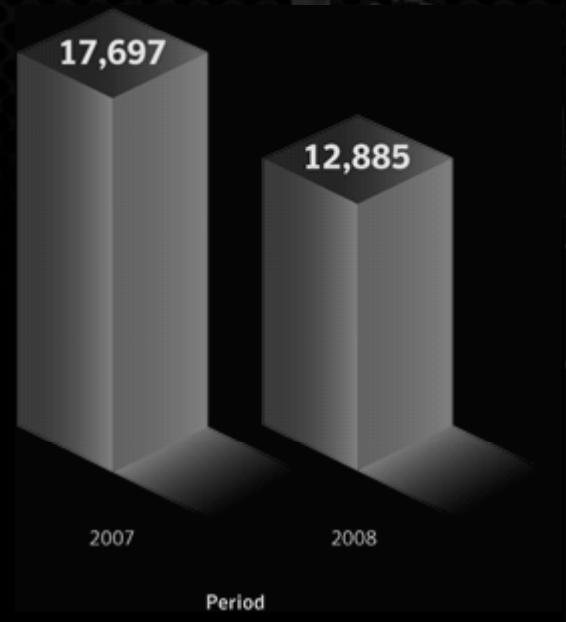
- Well-established infrastructure for monetizing stolen information

Rapid adaptation to security measures

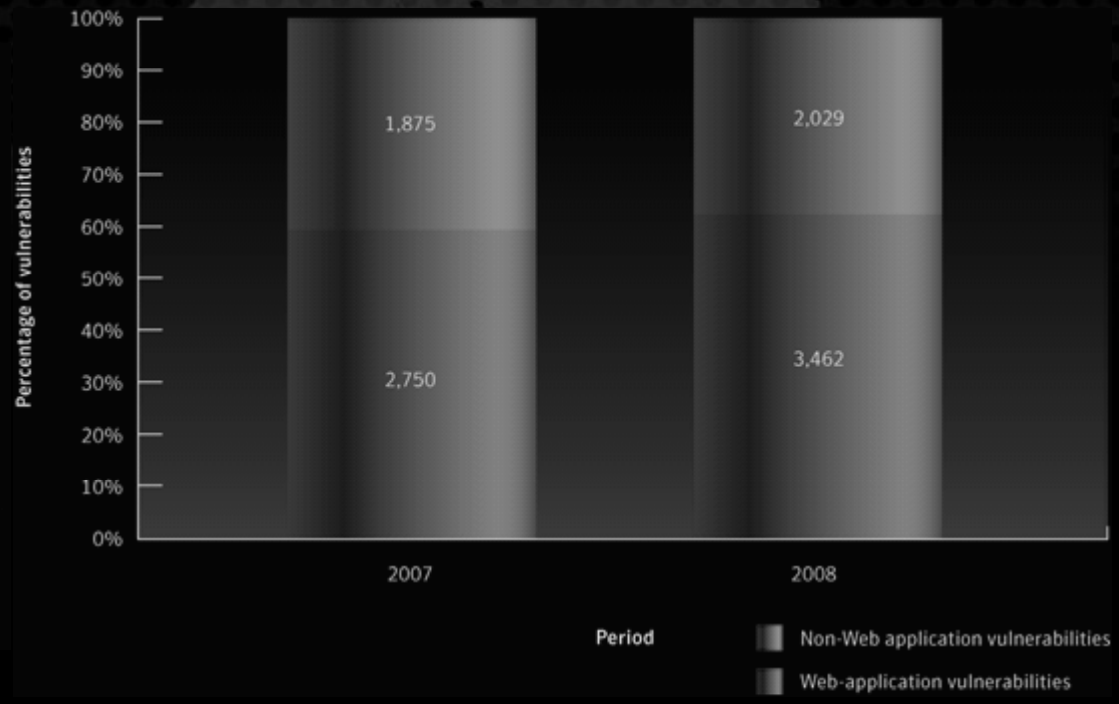
- Relocating operations to new geographic areas
- Evade traditional security protection

Web As The New Focal Point

- Attackers locate and compromise a high-traffic site through a vulnerability specific to the site or in a Web application it hosts.
- Once the site is compromised, attackers modify pages so malicious content is served to visitors.



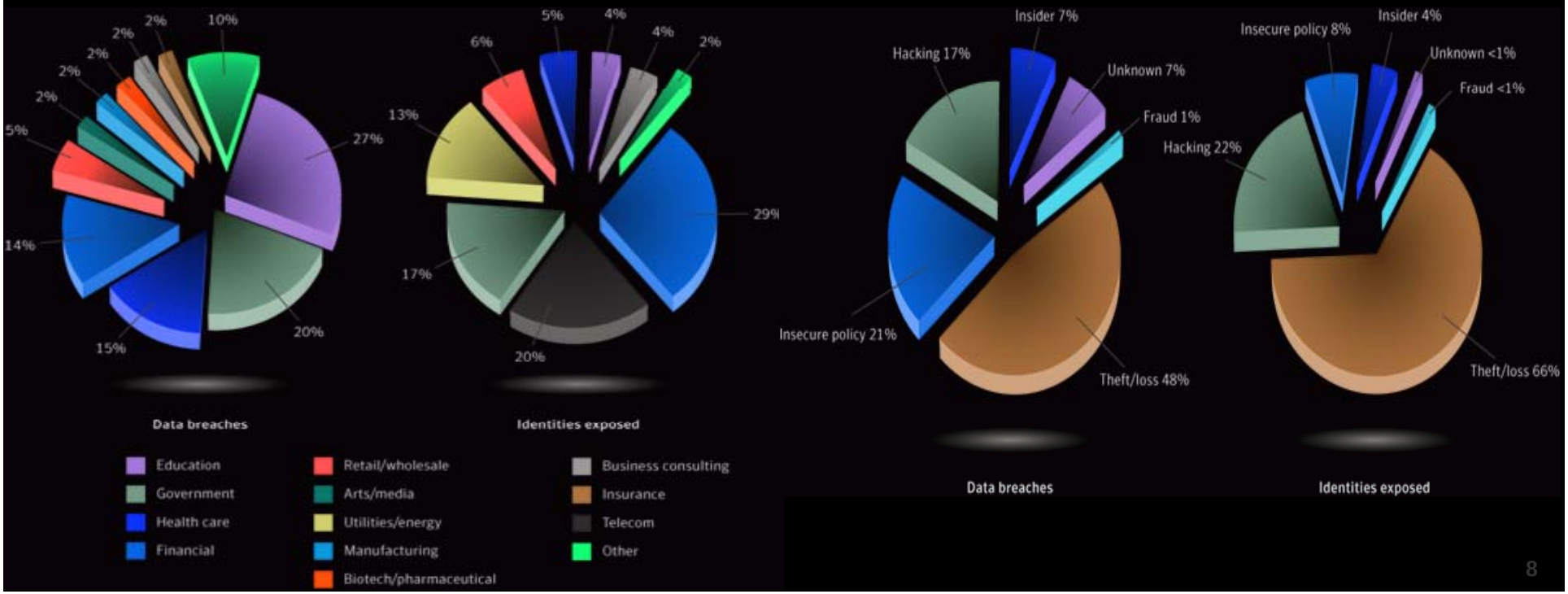
Site-specific vulnerabilities



Web application vulnerabilities

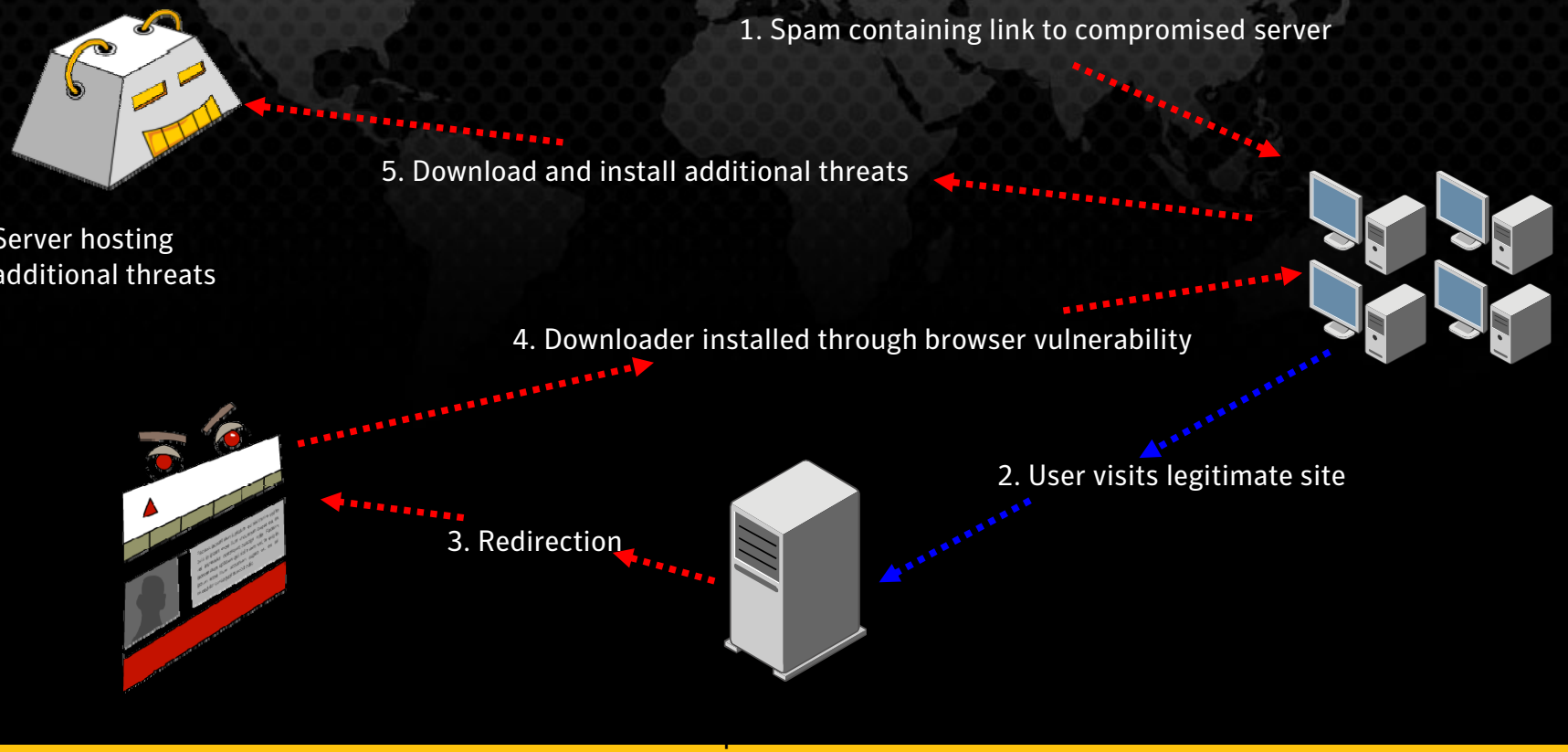
Information At Risk

- The Education sector accounted for the majority of data breaches with 27%, followed by Government (20%) and Healthcare (15%)
- More than half of breaches (57%) were due to theft or loss with insecure policy accounting for 21%.
- Many data breaches are related to loss of small, portable devices such as USB memory keys, portable hard drives, and smart phones.

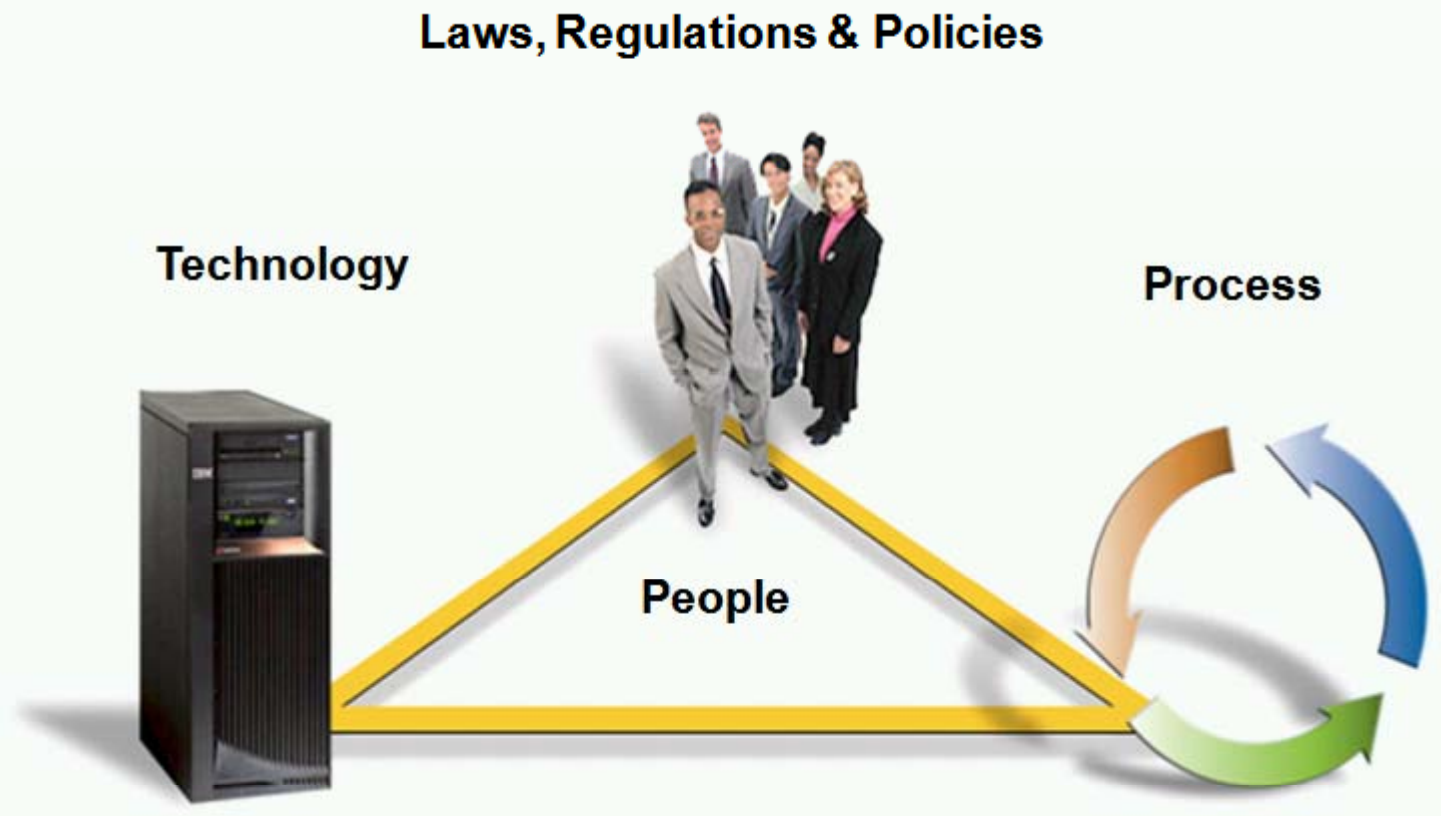


Convergence Of Attack Methods

Attackers combining malicious code, phishing, spam, exploitation of vulnerabilities, and online attacks

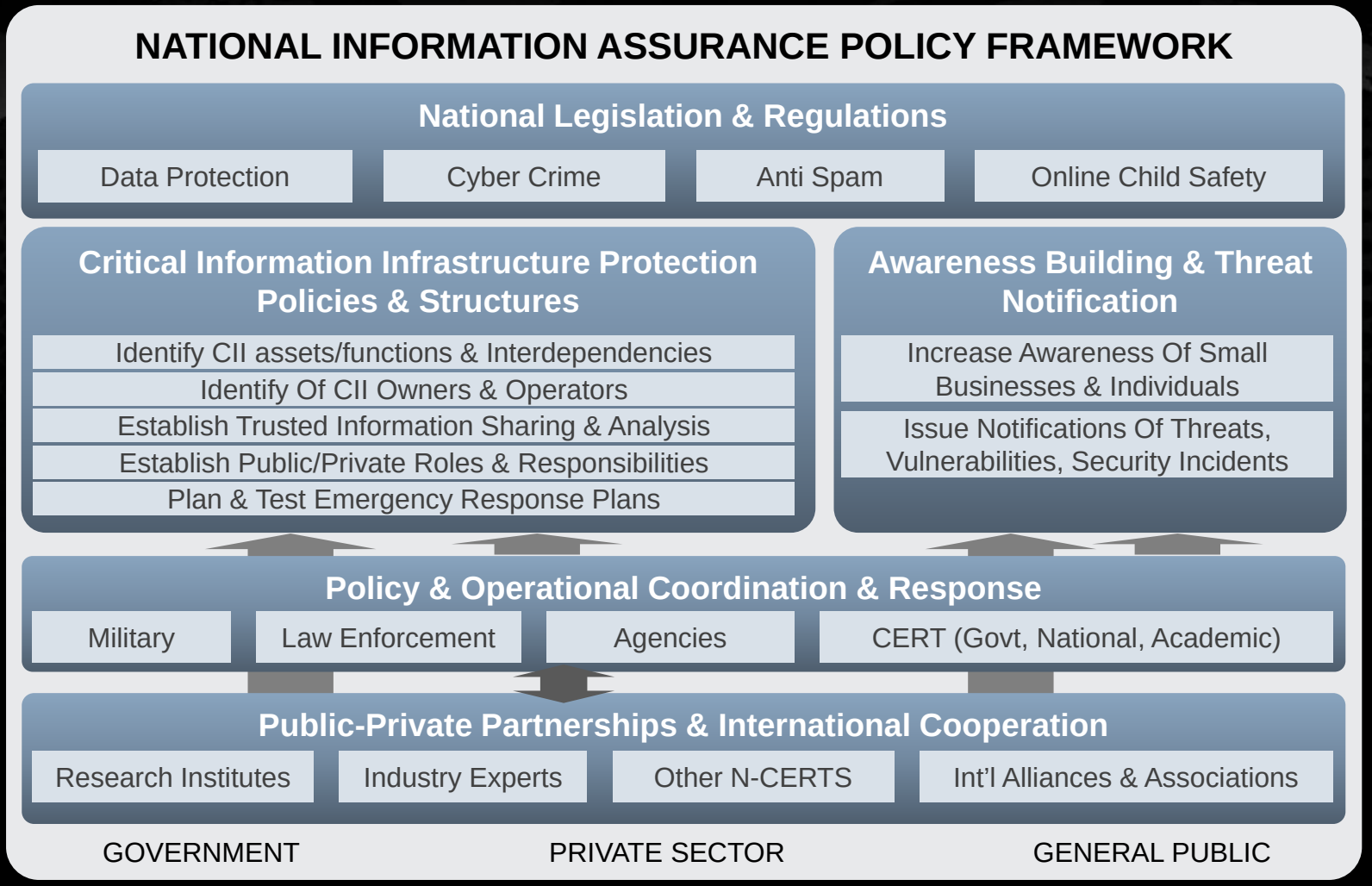


2>Establish Prioritised Risk-based Framework



Technology	People	Process
Multi-tier protection Endpoint protection & management Sensors & correlation Dashboard monitoring	Maintain adequate staff levels Recruit, train, certify & retain security specialists Increase security awareness amongst users and the public	Present & future threat analysis Incident response & recovery Pre-emptive protective measures Coordinate with international community & related bodies

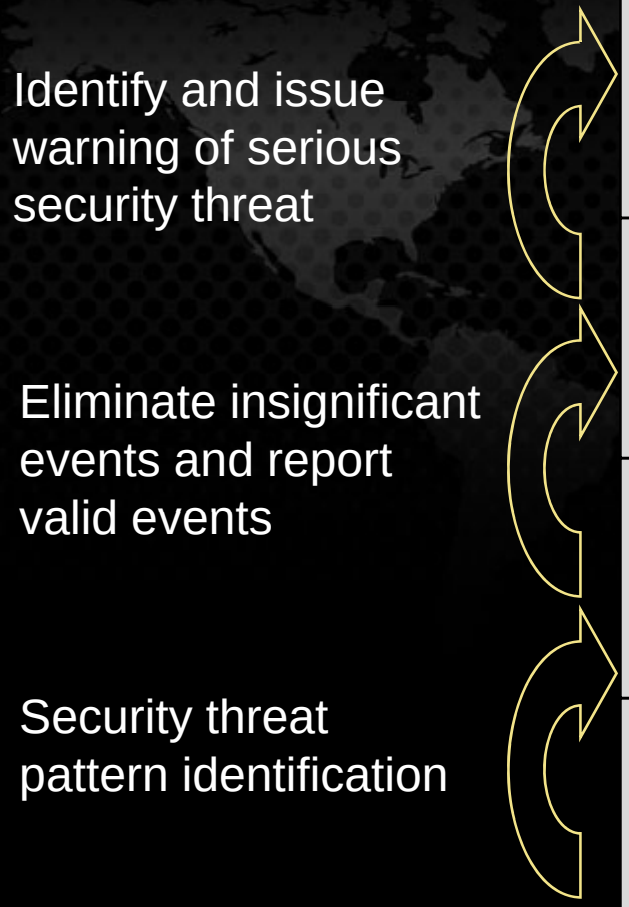
Information Assurance Framework



Fundamental Questions to Ask

- How are you keeping up?
- How much time does your staff invest in researching effective remediation best
- Are you leveraging the information you have?
- these resources?
- Are you optimizing your resources?

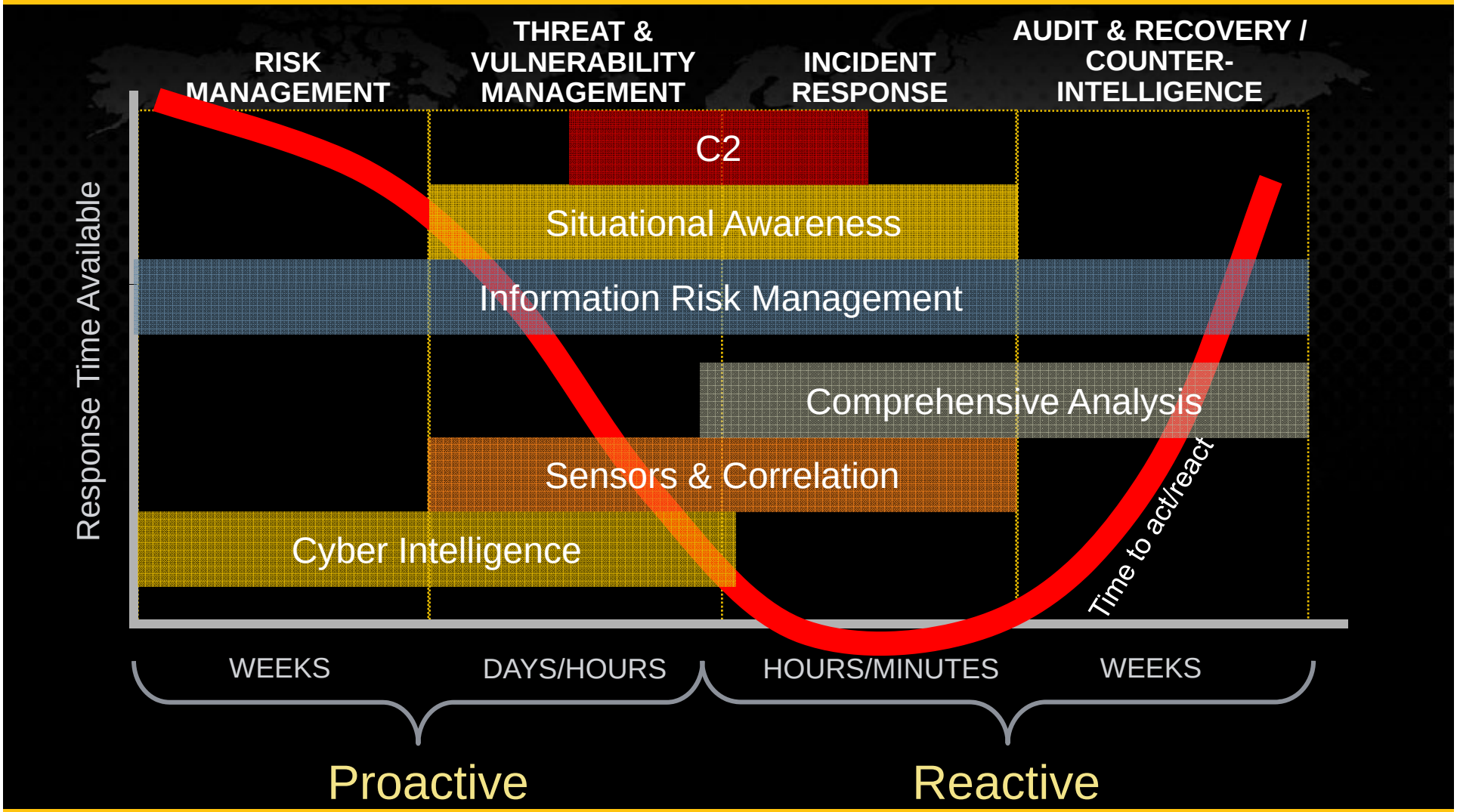
Prioritization A Constant Challenge



2	**Events Requiring Immediate Customer Contact**
55	**Events Provided for Client Review**
620	**Security Events**
9,481,668	**Logs and alerts generated by firewalls and IDSs**

Based on one month of actual customer data.

Risk-Based Approach



3>Develop Intelligence-in-Depth

Strategic Intelligence

- **GUIDANCE AND SUPPORT IN DEVELOPING AND MAINTAINING IA POLICY**
  - Strategic threat trend reports (ISTR)
  - Sector specific reports
  - Technology vulnerability assessments
  - Penetration testing
  - Environmental assessments

Operational Intelligence

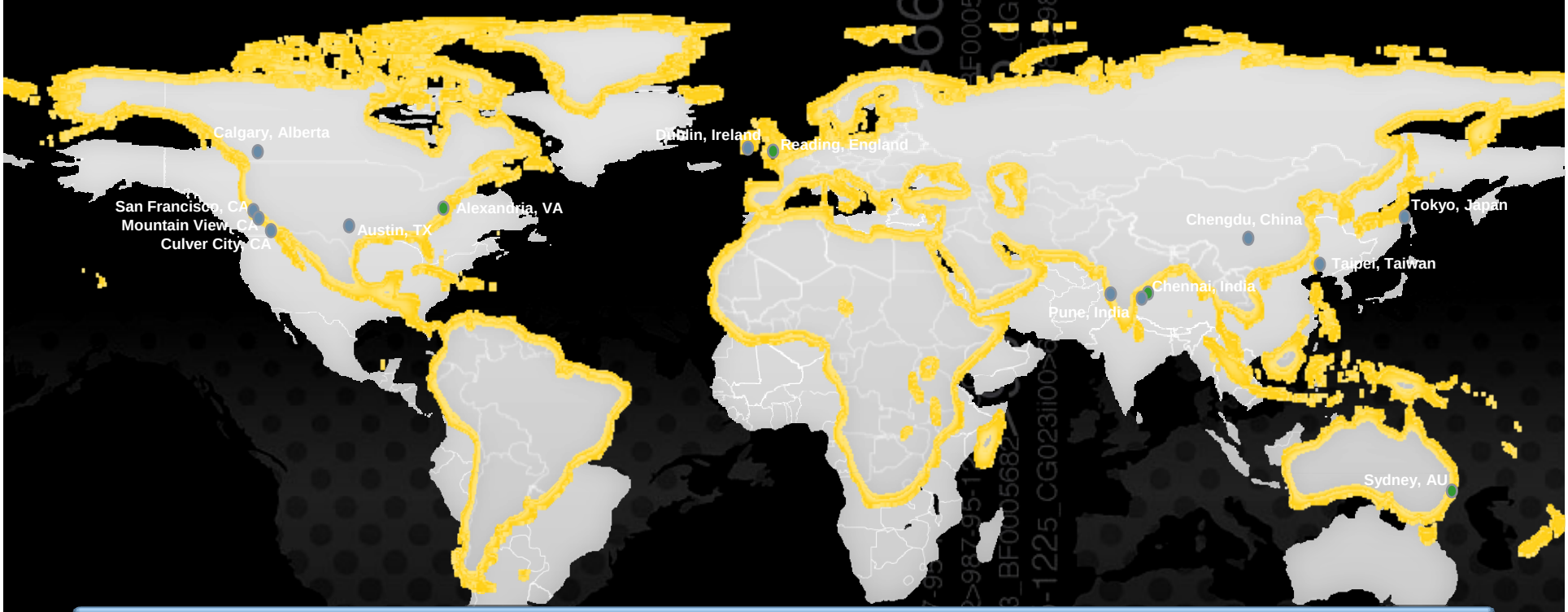
- **DELIVERY OF SITUATIONAL AWARENESS OF IA ACTIVITIES**
  - In depth analysis of targeted malware and attacks
  - Monitoring of network relevant vulnerabilities and exploits
  - Ongoing behavioural anomaly base lining and detection
  - Incident analysis and lessons learned
  - War gaming of potential attack vectors

Tactical Intelligence

- **TIMELY AND RELEVANT DELIVERY OF EVALUATED INTELLIGENCE TO ENABLE REAL TIME DECISIONS IN HANDLING AN INCIDENT**
  - Visual representation of suspicious activity and prediction of likely attack paths
  - Prioritisation of threats based on information and infrastructure criticality
  - Presentation of appropriate remediation methods to defeat attacks

Global Intelligence Network

Identifies more threats, takes action faster & prevents impact



Worldwide Coverage — **Global Scope and Scale** — 24x7 Event Logging

Rapid Detection

Threat Activity
- 240,000 sensors
- 200+ countries

Malcode Intelligence
- 130M client, server, gateways
- Global coverage

Vulnerabilities
- 32,000+ vulnerabilities
- 11,000 vendors
- 72,000 technologies

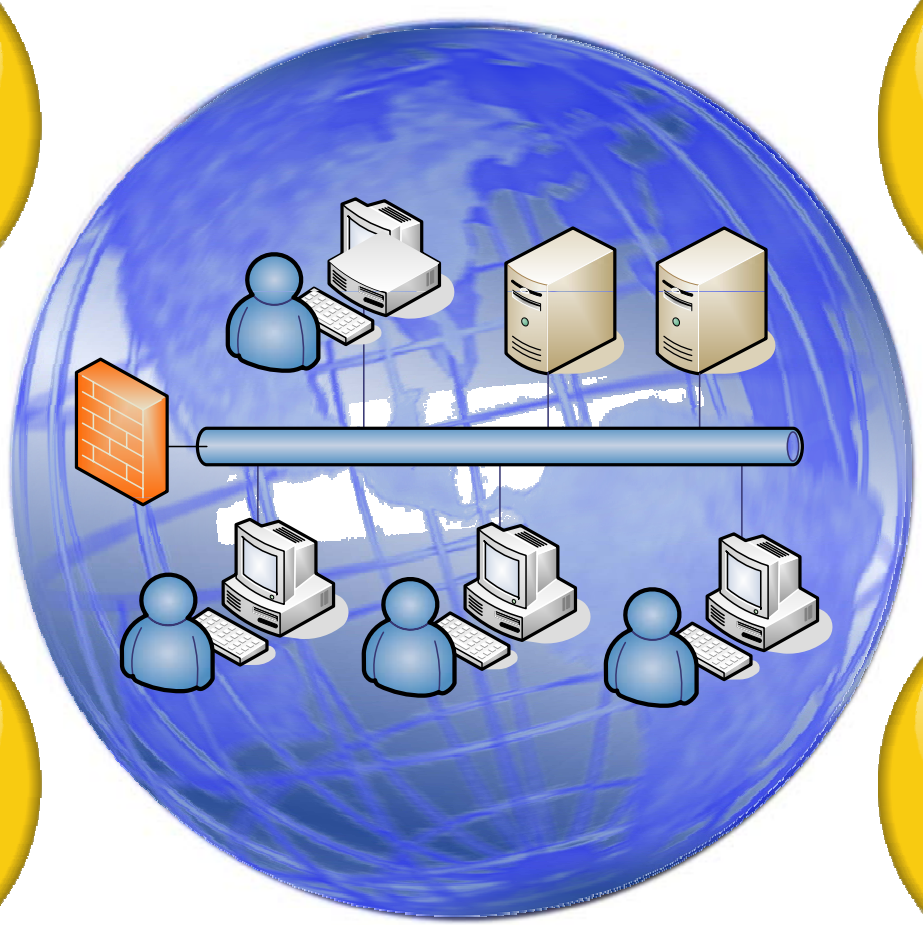
Spam/Phishing
- 2.5M decoy accounts
- 8B+ email messages/daily
- 1B+ web requests/daily

Preemptive Security Alerts — **Information Protection** — Threat Triggered Actions

Combining Global, Sector & Local Intelligence

Global Cyber Intelligence

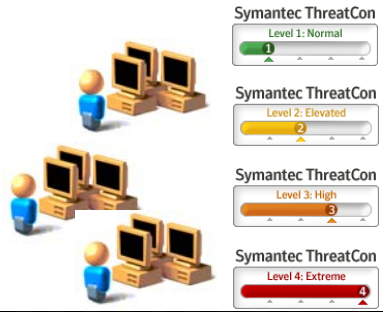
Global Real World Intelligence



Trusted Information Sharing

Local Network Information

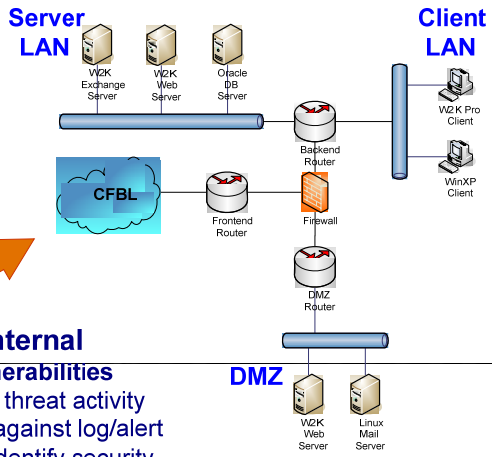
Security Event Monitoring & Correlation



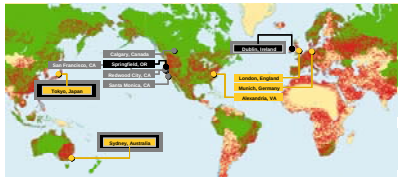
Alerts & Reporting
To NOC's and Users

Event Correlation
On internal vulnerabilities, global threat landscape, internal and external threat activity

Information Assurance Operations Centre

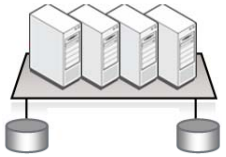


Internal Vulnerabilities
Internal threat activity analysis against log/alert data to identify security incidents



Response Labs
For Deep Analysis and Forensics

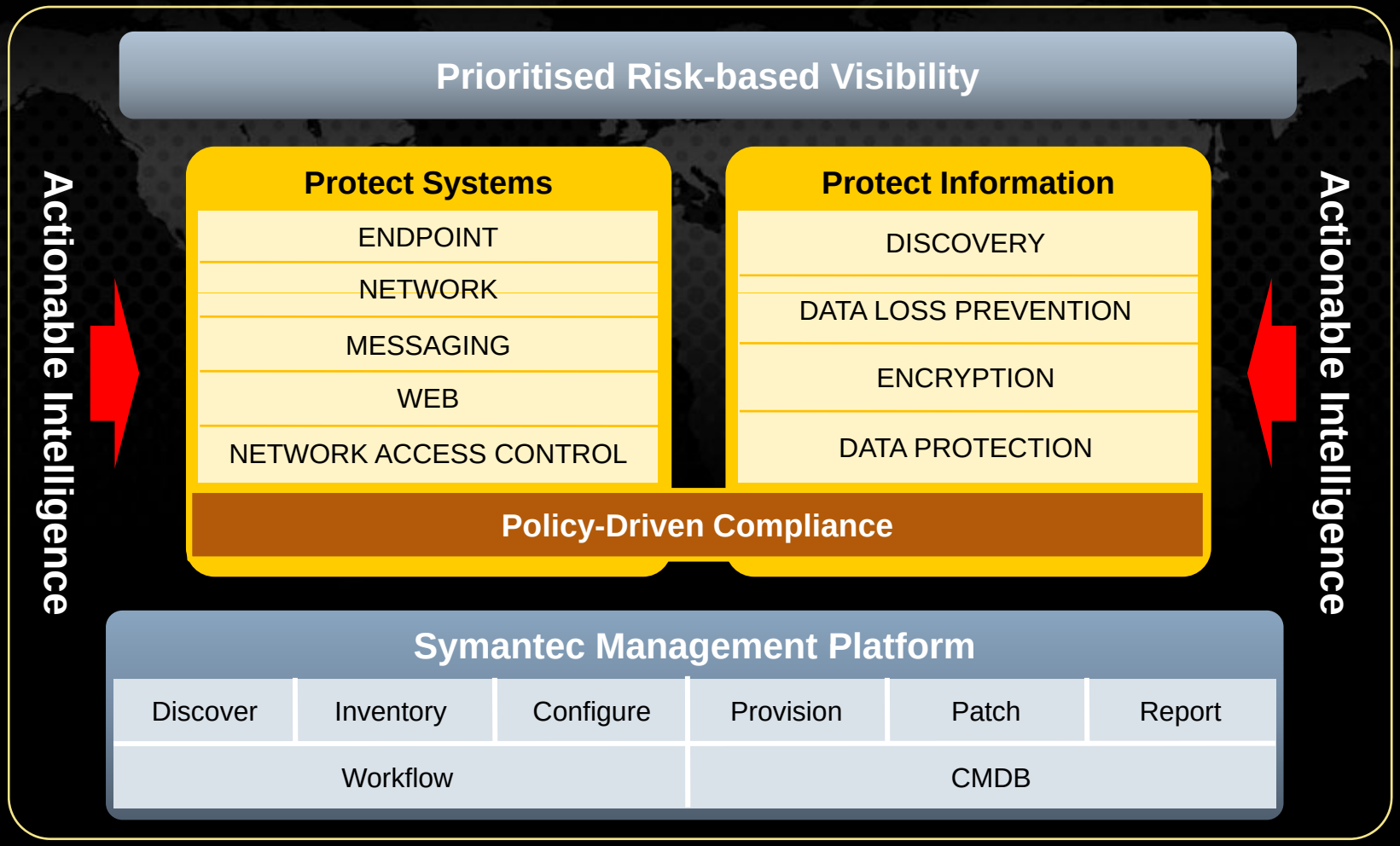
Global Security Intelligence
Vulnerabilities
Malicious Code
Early Warning
Threat Information
(Real time database feed)



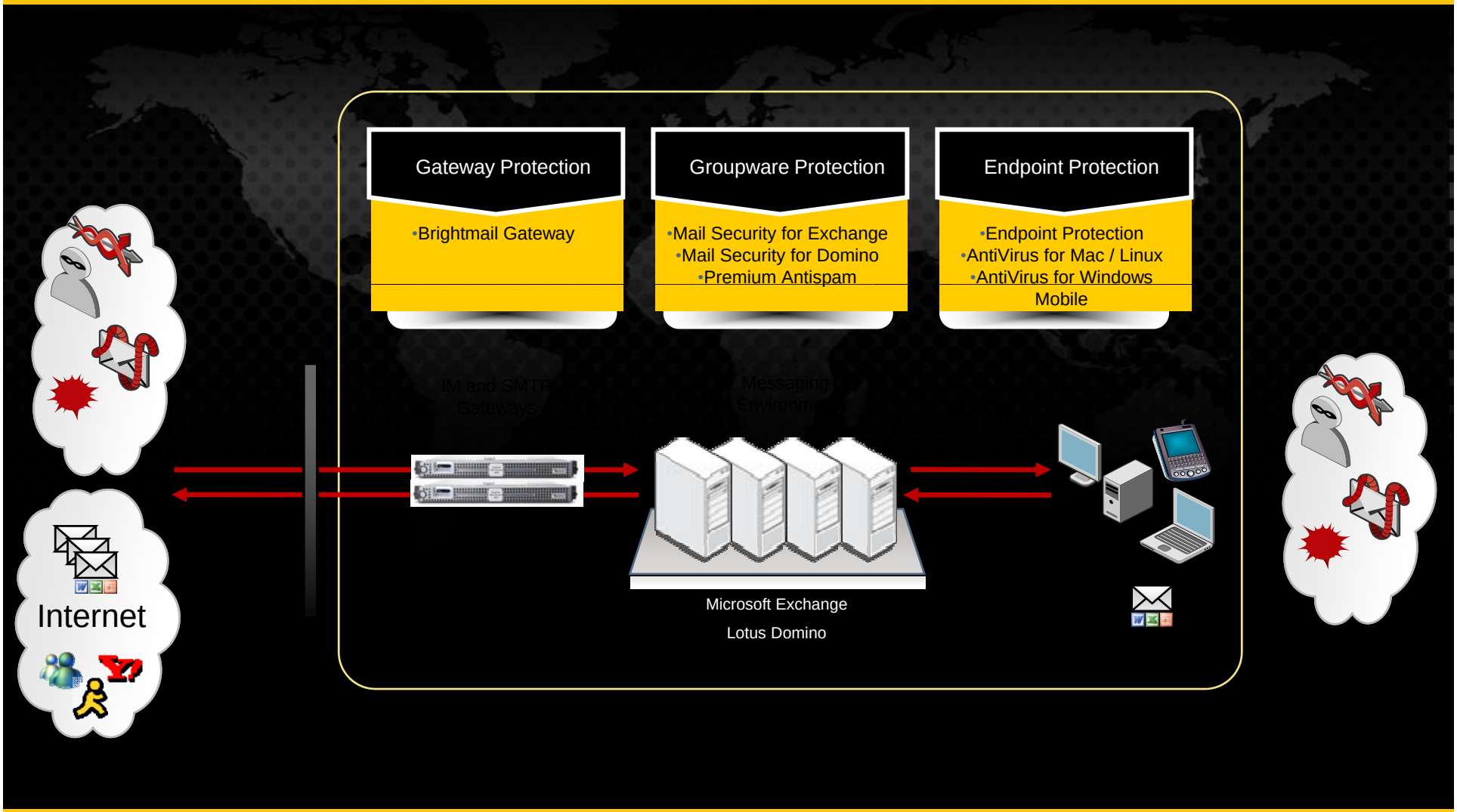
Live Update
Regular Live Updates to ensure that best Patch State is maintained

DeepSight™ Threat Management

4>Develop Strong Defense Capabilities



Multi-Tier Protection



Defending & Managing The Endpoints

Symantec Endpoint Protection

Threat Protection

Keep the Bad things Out

- Protect against malware
- Protect from known and unknown threats
- Manage multiple endpoint technologies

Symantec Network Access Control

Network Access Control

Trust, but Verify

- Enforce Endpoint Security policies
- Allow guest access to the network
- Provide access only to properly secured endpoints

Vontu DLP & Symantec Endpoint Encryption

Data Loss Prevention & Encryption

Keep the Good things In

- Discover confidential data
- Monitor its use
- Enforce policies to prevent its loss
- Encrypt to prevent unauthorized access

Altiris Client Management Suite

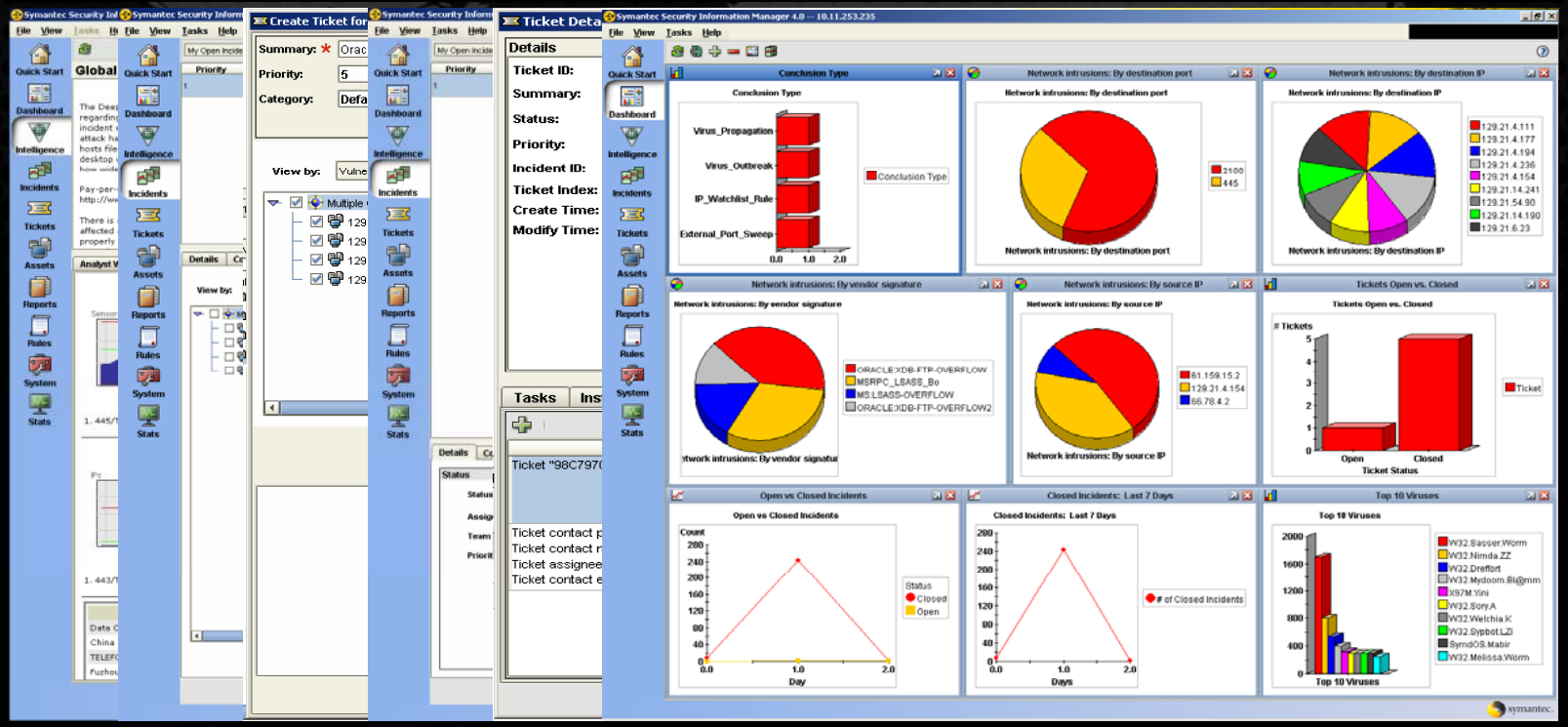
Endpoint Management

Keep the Wheels On

- Integrates security, data loss and management
- Provides automation
- Increases visibility and control
- Lowers total cost of ownership by managing multiple endpoint technologies

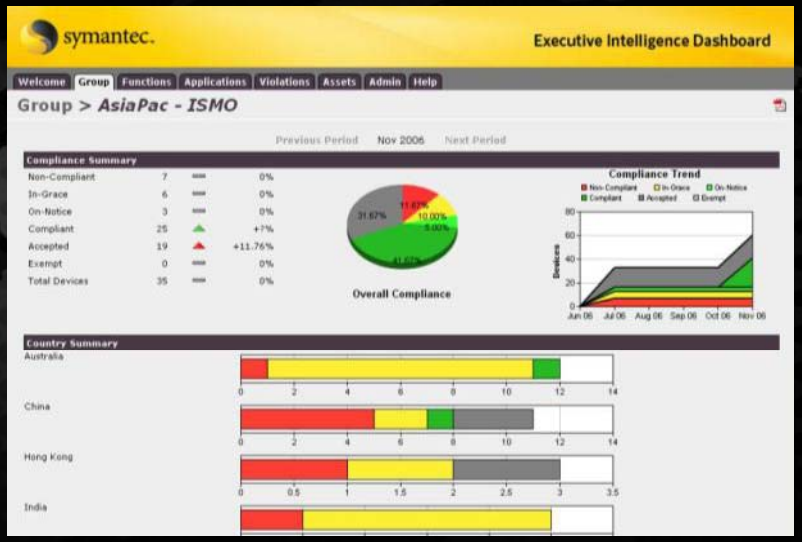
Sensor Deployment & Correlation

Monitor & Correlate → **Incident Actionable Alerts** → **Initiate Remediation Workflow** → **Helpdesk Processes** → **Security & IT Compliance Reports**



Symantec Security Information Manager (SSIM)

Executive Dashboard Monitoring



E.g. Vulnerability Assessment Module

Vulnerability information is collected and collated with organisation & asset info.

The analyst team is able to monitor status at a glance and drill down by theatre to individual assets. They can view trends and search for the status of any system.

Thank You!

Tan Wei Ming

weiming_tan@symantec.com

+65 96236998