
Osama Al-Zoubi
Senior Manager, Systems Engineering

Fahad Aljutaily
Senior Solution Architect, Security
Market Trends
Welcome to the New World
We Are Entering a New Era… Welcome to the New World…

80 billion connected devices by 2020

99% of “things” are unconnected

5 connected devices for every user by 2020

The Network Is the Platform to Connect the Previously Unconnected

Every company becomes a Technology company, every company becomes a security company

Cisco Connect, Riyadh, Saudi Arabia, April 29-30, 2014
### Connect the Unconnected …..Mobility Changes Everything!

<table>
<thead>
<tr>
<th>Mobile traffic increasing</th>
<th>50+% will be wireless by</th>
</tr>
</thead>
<tbody>
<tr>
<td>13X by 2017</td>
<td>2015</td>
</tr>
</tbody>
</table>

#### Cisco’s total mobile device count grew 109% in 24 months.

Last year’s mobile data usage was eight times the size of the Internet in 2000.

Mobile data traffic grew 159%.

Tablets will generate almost as much data in 2016 as the entire global mobile network in 2012.

---

“Mobility is More than Just the Device”

Mobility is to get complete control over a dynamic, mobile environment.

---

**Jan 2010**
- I want an iPhone with email, calendar, and contacts.

**Jan 2011**
- I want WebEx Meeting Center and Jabber IM on my iPhone.

**Jan 2012**
- I want AnyConnect and enterprise apps.

---

*Cisco Connect, Riyadh, Saudi Arabia, April 29-30, 2014*
Cloud Computing

69% of total data center traffic will be Cloud traffic by 2017.

Personal cloud traffic from 1.7 EB in 2012 to 20 EB in 2017.

Machine to Machine Connections is expected to grow 5 times.
Enormous, Fast, and Complex
Everything is generating data... Big Data

1 Trillion sensors - 150 for every person on Earth, By 2030

Big data is doubling the digital universe every 2 years

Growth of the Digital Universe

10^27
10^24

2012 Digital Universe
2030 Digital Universe

1,000x

Characteristics that define Big Data

Value
Variety
Volume
Velocity

Enormous
Fast
Complex

Digital Universe
2012
2030

Volume

Value

Variety

Velocity

Big data is doubling the digital universe every 2 years

Enormous, Fast, and Complex
Everything is generating data... Big Data

1 Trillion sensors - 150 for every person on Earth, By 2030

Big data is doubling the digital universe every 2 years

Growth of the Digital Universe

10^27
10^24

2012 Digital Universe
2030 Digital Universe

1,000x

Characteristics that define Big Data

Value
Variety
Volume
Velocity

Enormous
Fast
Complex

Digital Universe
2012
2030

Volume

Value

Variety

Velocity

Big data is doubling the digital universe every 2 years

Enormous, Fast, and Complex
Everything is generating data... Big Data

1 Trillion sensors - 150 for every person on Earth, By 2030

Big data is doubling the digital universe every 2 years

Growth of the Digital Universe

10^27
10^24

2012 Digital Universe
2030 Digital Universe

1,000x

Characteristics that define Big Data

Value
Variety
Volume
Velocity

Enormous
Fast
Complex

Digital Universe
2012
2030

Volume

Value

Variety

Velocity

Big data is doubling the digital universe every 2 years

Enormous, Fast, and Complex
Everything is generating data... Big Data

1 Trillion sensors - 150 for every person on Earth, By 2030

Big data is doubling the digital universe every 2 years

Growth of the Digital Universe

10^27
10^24

2012 Digital Universe
2030 Digital Universe

1,000x

Characteristics that define Big Data

Value
Variety
Volume
Velocity

Enormous
Fast
Complex

Digital Universe
2012
2030

Volume

Value

Variety

Velocity

Big data is doubling the digital universe every 2 years
New Work Environment, New Security Challenges

Today's dynamic computing environment creates new attack vectors.
Threat Evolution
Sophisticated, Enormous, and Complex
The Security Problem

- Changing Business Models
- Dynamic Threat Landscape
- Complexity and Fragmentation
The Industrialization of Hacking

- 1995: Phishing, Low Sophistication
- 2000: Hacking Becomes an Industry
- 2005: Sophisticated Attacks, Complex Landscape
- 2010: Spyware and Rootkits (2005–Today)
- 2015: APTs Cyberware (Today +)

Cisco Connect, Riyadh, Saudi Arabia, April 29-30, 2014
New Threat Landscape

- 52% of breaches affecting all organizations involved hacking.
- 40% incorporated malware.
- 70% of breaches were discovered by external parties who then notified the victim.
- $1T/year private sector revenue loss from cyber espionage.
- 75% driven by financial motives.
- 66% took months or more to discover.
- 76% of network intrusions exploited weak or stolen credentials.
- 75% are considered opportunistic attacks.
- 40% of breaches are Malware.
- 52% of breaches are Hacking.
Our Vision

Agile Security.... Security For The New World

New security model primed for toughest customer challenges
Supreme talent & innovative portfolio elements
Protecting your Safety, Security and Reputation
The New Security Paradigm

- Technology
- Monitoring / Engagement
- Security Operation
- Incident Response
- Policies
- People
The New Security Paradigm

- Technology
- People
- Monitoring / Engagement
- Policies
- Security Operation
- Incident Response

Cisco Connect, Riyadh, Saudi Arabia, April 29-30, 2014
Security is a Process… Enterprise Security Program Model

- You need to have a program and a framework to work within.
- This is from O-ESA:
  - Four rings = Four domains
  - Each domain is made of a number of activities/processes.
  - Comprehensive and deployable
  - Open
Security is a Process…
Enterprise Security Architecture

O-ESA
Enterprise Security Program Framework

Cisco Connect, Riyadh, Saudi Arabia, April 29-30, 2014
Security is a Process… Information Security Management System (ISMS)

Management Approval and Support
Supporting Organizational Structures (Roles, committees, staffing, knowledge, …etc.)

Policies, Standards, Procedures, Guidelines
Risk Management, Controls
Audit, Awareness
Processes, People, Technology

ISMS

Build, Implement, Operate, Optimize
Strategy

Cisco Connect, Riyadh, Saudi Arabia, April 29-30, 2014
Security is a Process…
The Incident Response Policy

- Should be part of your incident response preparation phase.

<table>
<thead>
<tr>
<th>Incident Response Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statement of management commitment</td>
</tr>
<tr>
<td>Purpose</td>
</tr>
<tr>
<td>Scope</td>
</tr>
<tr>
<td>Definitions</td>
</tr>
<tr>
<td>Organizational structure and identification of roles, responsibilities, and levels of authority</td>
</tr>
<tr>
<td>Prioritization or severity ratings of incidents</td>
</tr>
<tr>
<td>Effectiveness measures</td>
</tr>
</tbody>
</table>
Security is a Process…
Using technology to deliver on Policy Requirement…

**Desired Policy**

- Who can talk to whom
- Who can talk to which systems
- Which systems can talk to other systems

<table>
<thead>
<tr>
<th></th>
<th>Patient Records</th>
<th>Employee Intranet</th>
<th>Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doctor / Laptop</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Doctor / iPad</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Guest / Laptop</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Guest / iPad</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
</tbody>
</table>

**Simplifies policy implementation**

**Enhances security and reduces complexity**

**Accelerates Server Provisioning**

**Protect data by defining procedures, guidelines**

**Ensure that vulnerabilities are identified**
Security is a Process…
Using technology to deliver on Policy Requirement…

- Transform “plain English” rules into network policy
- Secure Access based on user, device, location, etc.
- Leverage TrustSec-enabled HW to enforce at ingress
- Securing access is more than simply deploying point solutions. In a rapidly changing environment, enterprises need an enterprise-class product from a strategic partner.
The New Security Paradigm
Information Security Awareness

Even the best information security policies, procedures, or controls are useless if employees are tricked not to follow them.

65% of companies and employees in the Middle East do not have the knowledge of the security risks.

Threats designed to take advantage of users’ trust in systems, applications, and the people and businesses they know are now permanent fixtures in the cyber world.
The New Security Paradigm
The New Security Model

**Survey**
Evaluate victim’s countermeasures

**Craft context-aware malware to penetrate victim’s environment**

**Execute**
Deploy malware. Move laterally, establish secondary access

**Check malware works & evades victim’s countermeasures**

**Accomplish**
The mission: Extract data, destroy, plant evidence, compromise.

- Deploy malware.
- Move laterally, establish secondary access.
- Evaluate victim’s countermeasures.
- The mission: Extract data, destroy, plant evidence, compromise.
The New Security Model

BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

Network
Endpoint
Mobile
Virtual
Cloud

Point in Time
Continuous
## Security Control Framework Model

### Total Visibility

**Identify, Monitor, Collect, Detect and Classify Users, Traffic, Applications and Protocols**

<table>
<thead>
<tr>
<th>Identify</th>
<th>Monitor</th>
<th>Correlate</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Identify, Classify and Assign Trust Levels to Subscribers, Services and Traffic</td>
<td>• Monitor Performance Behaviors, Events and Compliance with Policies</td>
<td>• Collect, Correlate and Analyze System-Wide Events&lt;br&gt;• Identify, Notify and Report on Significant Related Events</td>
</tr>
</tbody>
</table>

### Complete Control

**Harden, Strengthen Resiliency, Limit Access and Isolate Device, Users Traffic, Applications and Protocols**

<table>
<thead>
<tr>
<th>Harden</th>
<th>Isolate</th>
<th>Enforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Harden Devices, Transport, Services and Application&lt;br&gt;• Strengthen Infrastructure Resiliency, Redundancy and Fault Tolerance</td>
<td>• Isolate Subscribers, Systems and Services&lt;br&gt;• Contain and Protect</td>
<td>• Enforce Security Policies&lt;br&gt;• Migrate Security Events&lt;br&gt;• Dynamically Respond to Anomalous Events</td>
</tr>
</tbody>
</table>

---

Cisco SCF has been accepted as an industry standard
Architectural Approach
Comprehensive and Integrated

More Integrated Approach
The New Security Paradigm
Breaches Happen in Hours…
But Go Undetected for Months or Even Years

<table>
<thead>
<tr>
<th>Timespan of events by percent of breaches</th>
<th>Seconds</th>
<th>Minutes</th>
<th>Hours</th>
<th>Days</th>
<th>Weeks</th>
<th>Months</th>
<th>Years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Attack to Initial Compromise</td>
<td>10%</td>
<td>75%</td>
<td>12%</td>
<td>2%</td>
<td>0%</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>Initial Compromise to Data Exfiltration</td>
<td>8%</td>
<td>38%</td>
<td>14%</td>
<td>25%</td>
<td>8%</td>
<td>8%</td>
<td>0%</td>
</tr>
<tr>
<td>Initial Compromise to Discovery</td>
<td>0%</td>
<td>0%</td>
<td>2%</td>
<td>13%</td>
<td>29%</td>
<td>54%</td>
<td>2%</td>
</tr>
<tr>
<td>Discovery to Containment/Restoration</td>
<td>0%</td>
<td>1%</td>
<td>9%</td>
<td>32%</td>
<td>38%</td>
<td>17%</td>
<td>4%</td>
</tr>
</tbody>
</table>

In 60% of breaches, data is stolen in hours

54% of breaches are not discovered for months

Source: 2013 Data Breach Investigations Report, compiled by 18 organizations that contributed data
Visibility → Knowledge → Protection…
The New Security Paradigm

Technology

People

Policies

Monitoring / Engagement

Security Operation
Incident Response
Security Operation Centers Are Evolving...

1st Generation
- Device monitoring
- Log collection and retention
- Limited device coverage
- Slow reactions to incidents

2nd Generation
- Events correlation
- Network and system log collection
- Case management

3rd Generation
- Feeds from reputation services
- Vulnerability management
- Incident handling capabilities

4th Generation
- Big Data sophisticated security analytics
- Feeds from intelligence services
- Cloud processing
- Sophisticated NetFlow analysis
- Early alarming
- Forensics capabilities
<table>
<thead>
<tr>
<th>Facilities</th>
<th>Secure Facility</th>
<th>Open Space</th>
<th>Wall Screens</th>
<th>Separate areas for SOC Manager and meetings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure</td>
<td>Segregated</td>
<td>Secure</td>
<td>Highly Available</td>
<td>Collaboration Platforms</td>
</tr>
<tr>
<td>Services</td>
<td>Data Analysis</td>
<td>Anomaly Detection</td>
<td>Vulnerability Management</td>
<td>Collaboration platforms</td>
</tr>
<tr>
<td>People</td>
<td>Awareness</td>
<td>Reporting</td>
<td>Committee Involvement</td>
<td>Collaboration</td>
</tr>
<tr>
<td>Processes</td>
<td>Effective Incident Handling</td>
<td>Measurements and Metrics</td>
<td>Continues Enhancement</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Day 1 SOC</td>
<td>Accelerated Maturity</td>
<td>Threats will not wait for you to finish building your SOC!</td>
<td></td>
</tr>
</tbody>
</table>

Security Operation Centers ... For the new world
Security Operation Centers
Well-Defined Methodology…

Compliance
- Vulnerability Management
- Incident Management

Deployment
- Service
- Administration
- Event Management

Device and Applications

Device and Applications
- Compliance
- Vulnerability Management
- Incident Management
- Deployment
- Service
- Administration
- Event Management

Compliance
- Vulnerability Management
- Incident Management
Security Operation Centers
Well-Defined Methodology…

- Good practices exist today to help you develop your capabilities.
- Incident handling requires **people, process and technology**.

### Standards

- **ISO/IEC 27035:2011** Information technology -- Security techniques -- Information security incident management
- **ENISA** Good Practice Guide for Incident Management
- **NIST SP 800-61 Rev. 2** Computer Security Incident Handling Guide
- **NIST SP 800-83 Rev. 1** Guide to Malware Incident Prevention and Handling for Desktops and Laptops.
- **ISO/IEC 27035:2011** Information technology -- Security techniques -- Information security incident management
- **Incident Response and Management: NASA** Information Security Incident Management
Security Operation Centers
Well-Defined Methodology…

Don’t build your incident handling plan during an incident.

Clearly identified Roles and responsibilities.

During an incident stick to the plan.

Run incident drills. Practice makes you better.

Involve members from different departments: IT, PR, Legal.

Communication with the rest of the organization. Whom, How and what?

Think about having something like a playbook!
The Incident Response Policy

- Should be part of your incident response preparation phase.

<table>
<thead>
<tr>
<th>Incident Response Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statement of management commitment</td>
</tr>
<tr>
<td>Purpose</td>
</tr>
<tr>
<td>Scope</td>
</tr>
<tr>
<td>Definitions</td>
</tr>
<tr>
<td>Organizational structure and identification of roles, responsibilities, and levels of authority</td>
</tr>
<tr>
<td>Prioritization or severity ratings of incidents</td>
</tr>
<tr>
<td>Effectiveness measures</td>
</tr>
</tbody>
</table>
Incident Handling – The Fundamental Steps

Life of an incident

SHORT TERM GOAL

LONG TERM GOAL

Preparation → Detection → Initial Response → Incident Investigation → Reporting → Post Incident Activities

Incident Investigation

Data Collection → Data Analysis

Containment
Recovery

SHORT TERM GOAL

LONG TERM GOAL

Cisco Connect, Riyadh, Saudi Arabia, April 29-30, 2014
Agile Cyber Security
Security for the Real World, Architectural Approach

The New Security Paradigm
Thank You