RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking

SESSION ID: SPO-W07B

Using Visibility To Turn The Tables on Cybercriminals

Johnnie Konstantas

Director, Security Solutions
Gigamon Inc.
Twitter: @jkonstantas

Agenda

- Turning the tables on cybercriminals
  - Visibility: the core of Cyber Network Defense (CND)
    - Your current security maturity model
    - Changing the assumption of safety
    - Transforming your approach to security
    - Architecting your security around CND
    - Filling out your CND action matrix
    - Making your network CND pervasive
    - Dealing with a very real “Big Data” problem
    - Pulling it all together:

      CND through Pervasive Visibility

RSAConference2015
Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: SPO-W07B

Recommendation 1

Understand Your Organization's Cyber-Security Maturity

Modelling Organizational Maturity

- How Organizations Approach Cyber-Security Threats

Organizational Security Maturity

Characteristics and Typical Behavioural Statements

Denial

Key Characteristic

There is no security problem

"We have nothing worth stealing"

"Nobody would be interested in us"

Product Focused

Key Characteristic

Security problems are solved by the correct product

"We installed <product name>, so we are safe"

"We have firewalls and anti-virus, so nobody can break in"

Compliance Focused

Key Characteristic

Conflate implementing a compliance with their organizational security requirements

"We spent hundreds of thousands of dollars implementing PCI:DSS. We're safe"

Risk Based

Key Characteristic

See security as a risk-management exercise, as a component of tgovernance, risk and compliance

"We don't talk about secure and insecure, we manage risk against our business objectives"

Security Operational

Key Characteristic

Security is an on-going operational process. May have focus on product assurance (esp. government and DIB)

"We know that attackers are probably in our network, our job is to find them and kick them out"

Strategy and Assumptions

“For most companies, it's not a matter of if, but a matter of when and how they will be attacked. We must learn to live under a constant state of compromise.

This does not mean we have to live in a constant state of loss.”

Tom Heiser, RSA COO, RSA Conference Europe (11th October 2011)

Recommendation 2

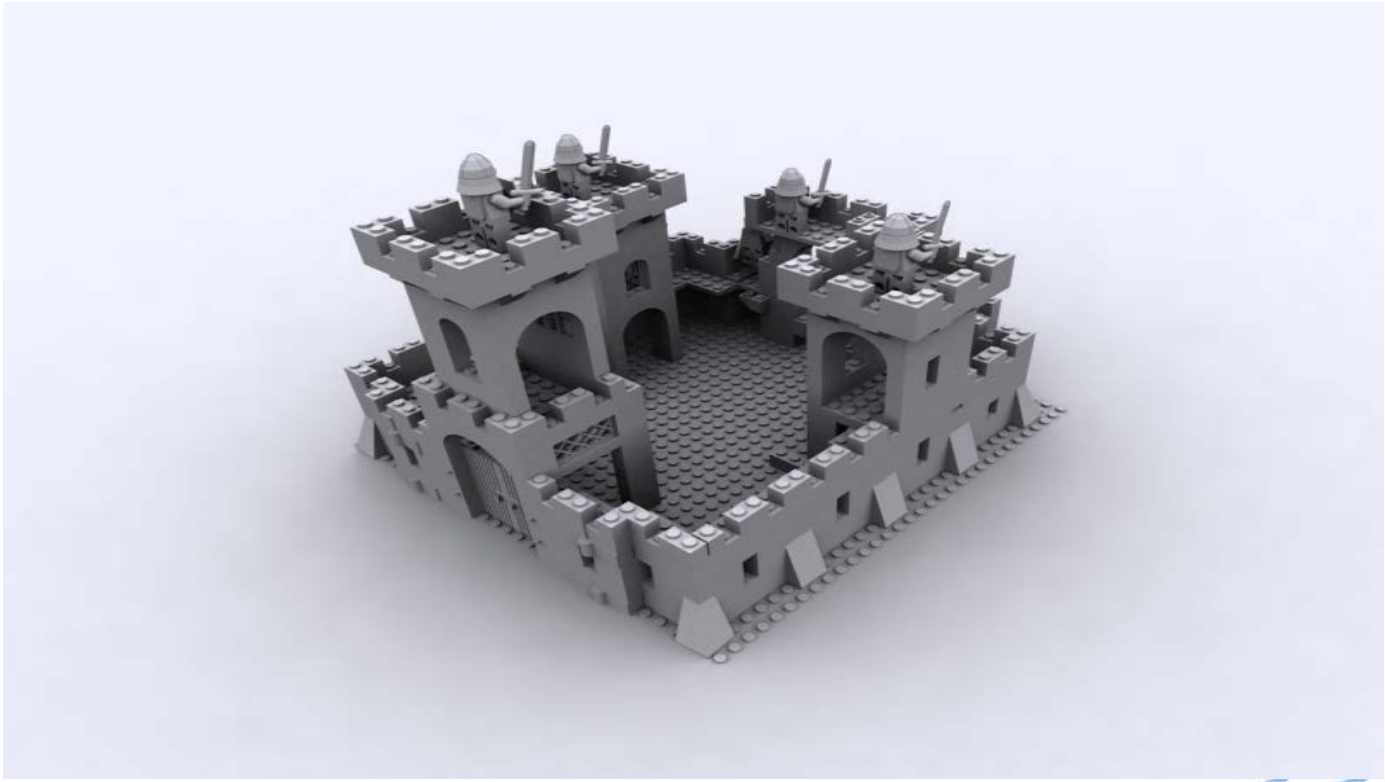
The Assumption of Compromise, and Operationalizing Security

Strategy and Assumptions

"We have to build our systems on the assumption that adversaries will get in"

Debora Plunkett – NSA Information Assurance Directorate (Dec 16th 2010)

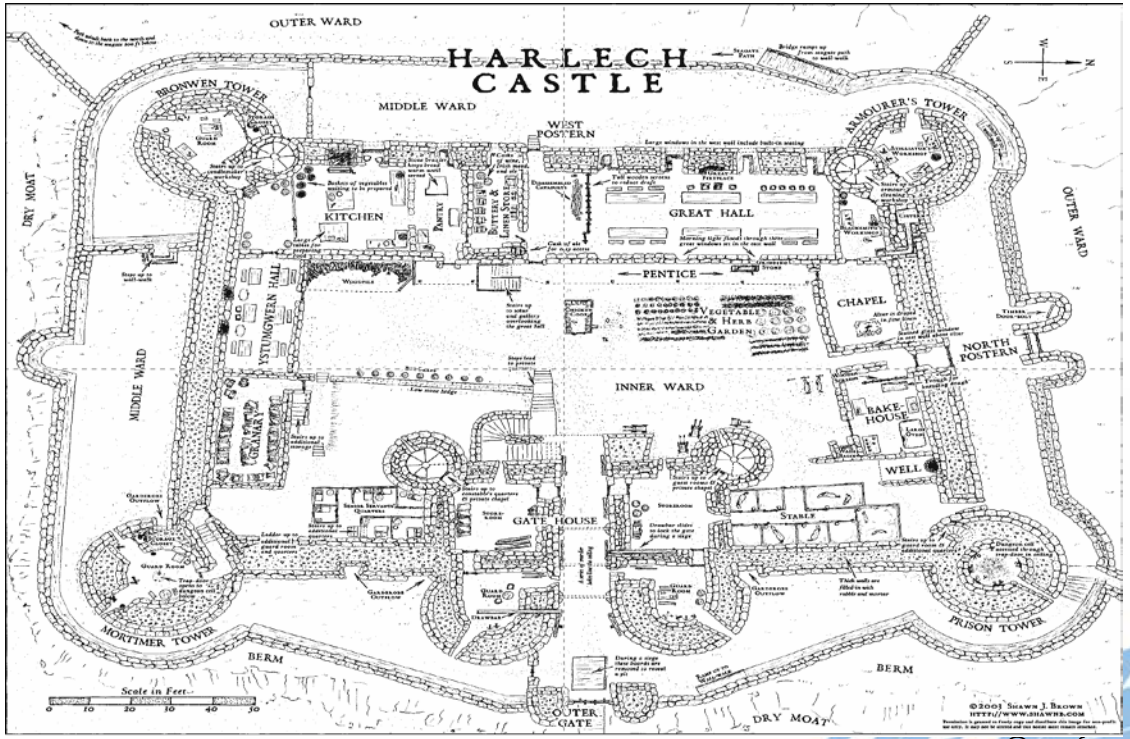
Castle-Moat Architectures



Castle-Moat Architectures

Real Medieval castles did not have a castle-moat architecture

- Real castles had:
  - Multiple wards (subnets)
  - Lots of choke points for attackers (internal firewalls)
  - Lots of high points for archers (visibility)
  - No implicit trust just because you were inside the walls (ie. understood “insider threats”)

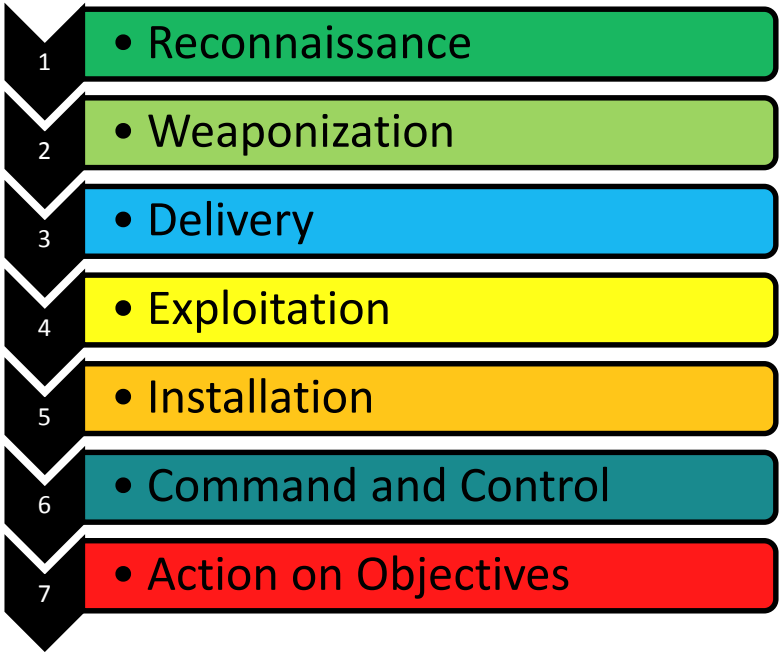


Recommendation 3

Implement the Kill Chain Model
or Equivalent Computer Network Defence (CND) Methodology

Computer Security Kill Chain Stages

- Understand the Stages to Disrupt an Attack



Harvesting internal information information from social media, conferences, public information, social engineering etc.

Coupling a viable exploit with a deliverable payload to be directed at the target

Delivering the weaponized bundle to the target via email, web, USB, CD/DVD, trojanized hardware etc.

The exploit is executed on the target system, where it exploits the vulnerability

The malware is installed on the asset (directly or via a dropper)

The malware communicates externally with the Command and Control (C2) server(s), announcing its success and allowing remote manipulation of the victim

With full access to the target system, the intruder moves laterally through the organization, achieving their desired objectives

Course of Action Matrix

Filling Out the Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web Analytics, OpSEC training for front-line staff, operational intelligence into darknet	WAF	Block access from unauthorized VPNs, TOR exit nodes, high-risk locations	OpSEC User Education (esp. around Social Media)	Social Media Honeypots	
Weaponization	NIDS	NIPS				
Delivery	OpSEC User Education and evaluation, Sandbox anti-malware, e-forensic Traffic Recording	Proxy Filter, Device Control software and/or hardware	In-line anti-malware, email encryption/authentication	Queuing	Ingress, parcel and mail redirection for high-risk items	
Exploitation	HIDS, SIEM	Configuration and patch management, HIPS, application whitelisting	DEP, ASLR, EMET, admin rights restrictions			
Installation	HIDS, Memory Analysis Agents	"chroot" jail/sandboxes	Anti-malware, Application Whitelisting	Disposable virtual desktops		
C2	NIDS, e-Forensic Traffic Recording, APM	Firewall, gateway blacklisting	NIPS, proxy "click-thru"	Tarpit	DNS redirect, blackholing	
Actions on Objectives	SIEM, e-Forensic Traffic Analysis	Network Segmentation with authenticated		Quality of Service	Honeypot	

Legend
Red = network-based
Black = host-based
Green = operational

Gigamon

Recommendation 4

Deploy Tools Pervasively Throughout the Network (Core to Edge)

Taxonomy of Security Tools

This list is not exhaustive…

- Authentication, Identity and Access Management
- Anti-Malware (“Anti-Virus”)
- Anti-Spam
- Application Security Testing
- Certificate Authorities and Cryp Mgmt
- Configuration Management
- Data Diodes and Cross-Domain Solutions
- Data Loss Prevention (DLP)
- Intrusion Prevention Systems (IPS)

- Messaging Encryption
- Messaging Security
- Document Discovery and Management
- File Activity Monitoring (FAM)
- Firewalls
- Governance, Risk and Compliance (GRC)
- Intrusion Detection Systems (IDS)

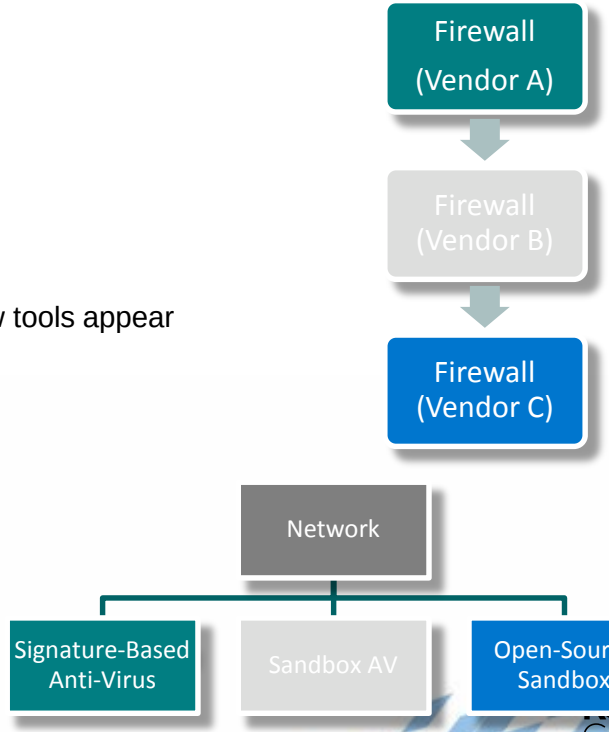
- Network Encryption
- Network Proxies
- etwork Forensics (Full Packet pture/Traffic Recorders)
- curity Analytics (SA)
- curity Information and Event anagement (SIEM)
- SSL Acceleration and Decryption
- Vulnerability Testing and Exploit Platforms
- Web Abuse/Web Fraud Detection (Web Session Intelligence)
- Web Application Firewalls (WAF)

Many non-security tools have security use cases (eg. APM for Shadow IT detection)

Strategic Tool Deployment

Be Realistic About Security Tool Capabilities

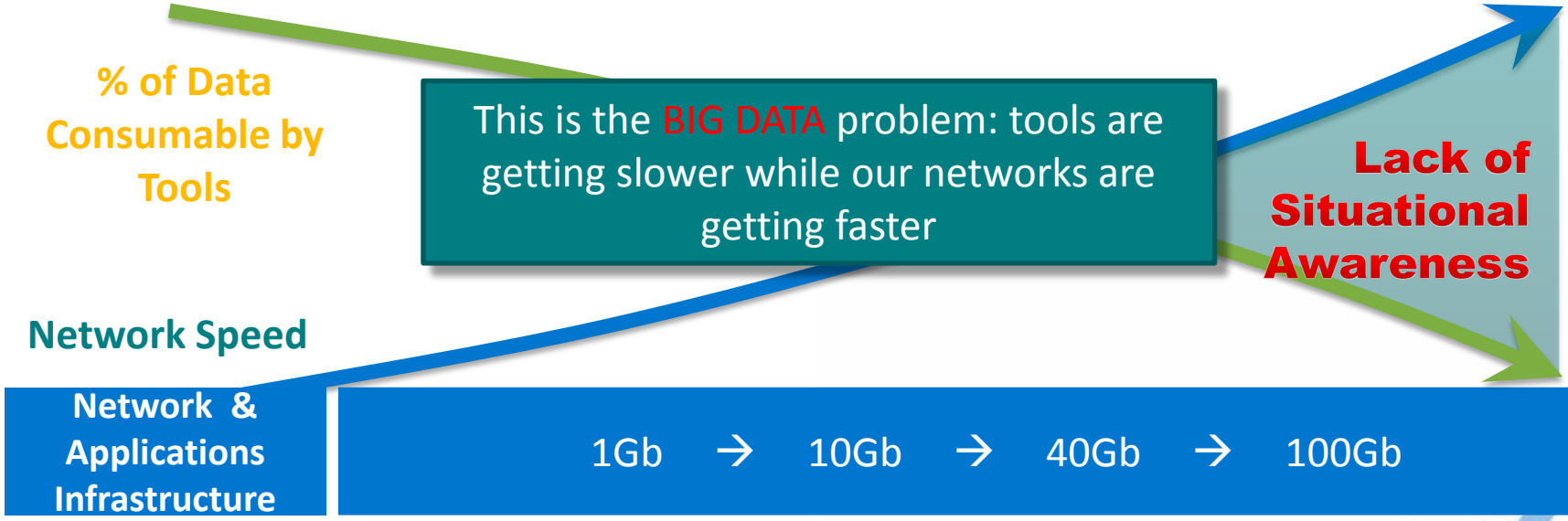
- Moving beyond single security tools:
  - Multiple tools deployed in series (inline)
  - Multiple tools deployed in parallel (out-of-band tools)
- Tool agility
  - Today's "hot tool" may be tomorrow's expensive "also ran"
  - Tool deployment becomes a constant evaluation of efficacy as new tools appear on the market and from open source
- Architect for tool failure
  - Physically (especially for inline)
  - Functionally
- Beware of tool performance stats
  - Just because it has a 10G port doesn't mean it can handle 10G at line-rates (actually, it can't on x86)



Gigamon

Gap in Data Volume and Relevancy

Security Tools → Signature- and Policy-Based → Advanced Analytics



Why Are Security Tools Getting Slower?

- Traditional tools detected “known bad”
  - Signature-based tools (traditional IDS, signature-based anti-malware)
  - Policy-driven (firewall)
  - Single algorithm typically used on an immediate data stream
- Advanced Security tools detect “suspected bad”
  - Deep Packet Inspection (FAM, DAM, WAF, e-forensic recorders)
  - Deep Content Inspection (DLP)
  - Anomaly detection, trend estimation, bayesian analysis,
- “Big Data” Security analytics – consolidating tool activity
  - 0-60 seconds: IOC/Signature detection of attack (inline/online only)
  - 0-15 mins: Sandbox alerting of malicious attack (inline/store-and-forward)
  - 0-60 mins: SIEM analysis (alerts and correlations)
  - 60 mins-1 week and beyond: trend analysism and reporting

...or...

Recommendation 5

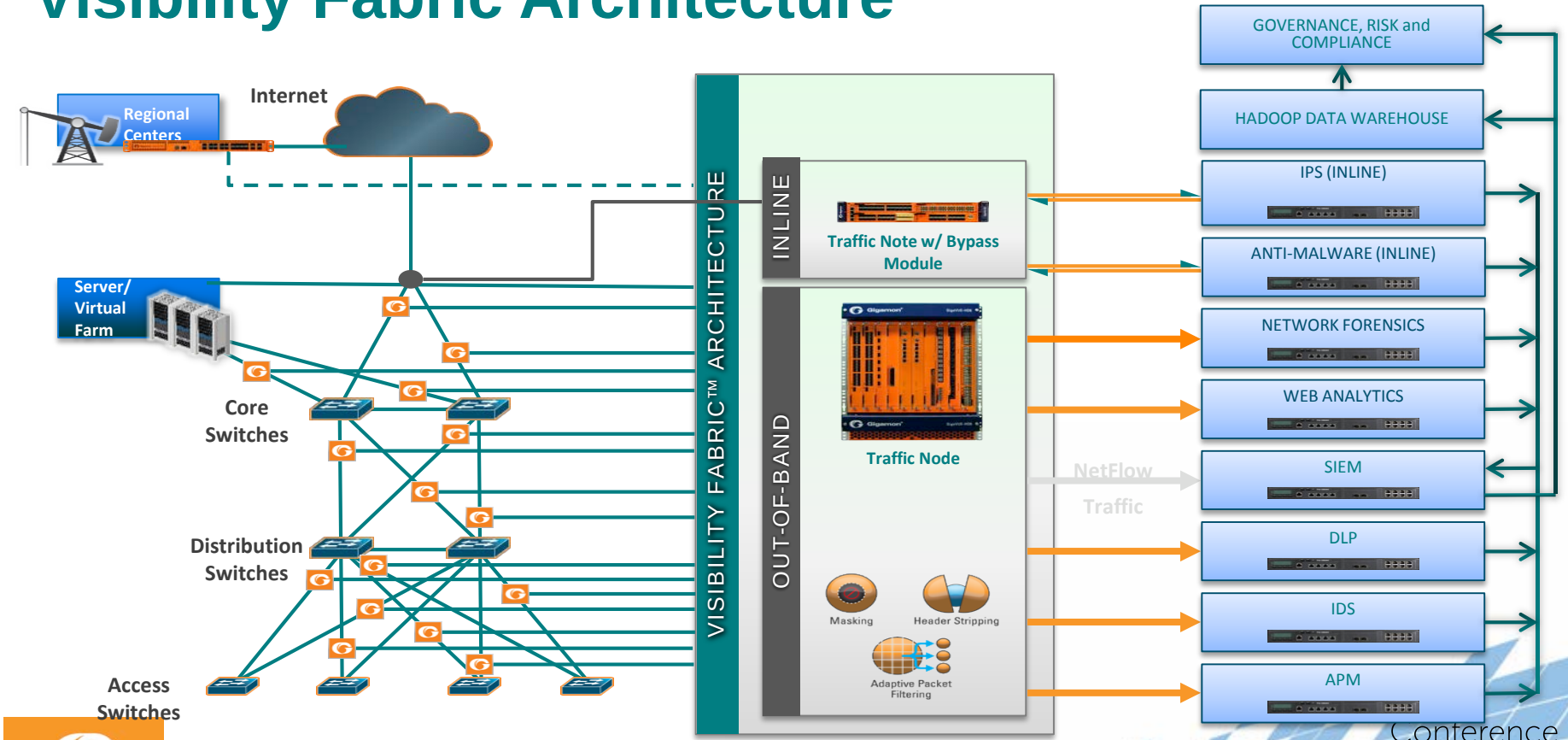
Implement Active Network Visibility for Multi-Tiered Security

Solution:
"Active Visibility" For Multi-Tiered Security

1. TAP all critical links
2. Connect links to a High Availability Visibility Fabric
3. Connect inline security tools
4. Connect out-of-band security tools
5. Leverage traffic intelligence
6. Add non-security tools to maximize ROI

Gigamon

Visibility Fabric Architecture



Evaluating the Outcomes

Recommendations	
1	Understand Your Organization's Cyber-Security Maturity
2	The Assumption of Compromise, and Operationalizing Security
3	Implement the Computer Security Kill Chain Model or Equivalent Computer Network Defence (CND) Methodology
4	Deploy Tools Pervasively Through-Out the Network (Core to Edge)
5	Implement Active Network Visibility for Multi-Tiered Security

QUESTIONS?