




# Continuous Vulnerability Monitoring for Internet Service Providers

Disney Cheng, Solutions Architect, Asia Pacific  
[dcheng@tenable.com](mailto:dcheng@tenable.com)

# Agenda

- The risk for ISPs/Data Centre Operators
  - The rate at which vulnerabilities emerge
  - Some examples of ISP compromise and the impact
  - The Continuous Vulnerability Management methodology
  - Benefits / conclusion
- 

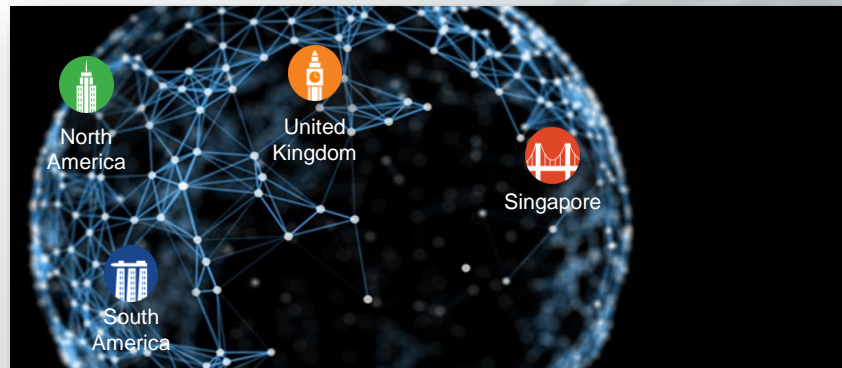
# About Tenable

## The Gold Standard for Continuous Network Monitoring

- Category-defining Platform
- Strong Positive Analyst rating
- Founded in 2002
- Best of Breed Technology
- Expert Executive & Technical Team
- 11 consecutive years of growth
- Award-winning Technology & Company



## 20,000+ Customers Worldwide Over 1 million Nessus users



# THE RISK FOR ISPS/DATA CENTRE OPERATORS

---

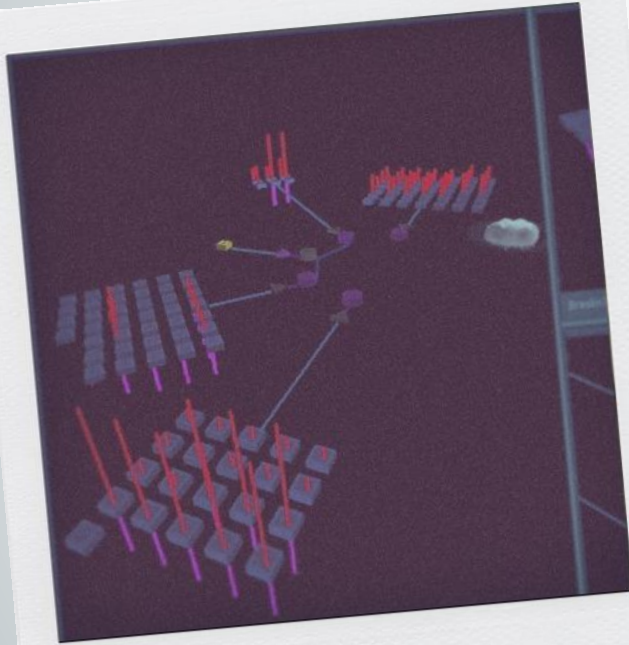




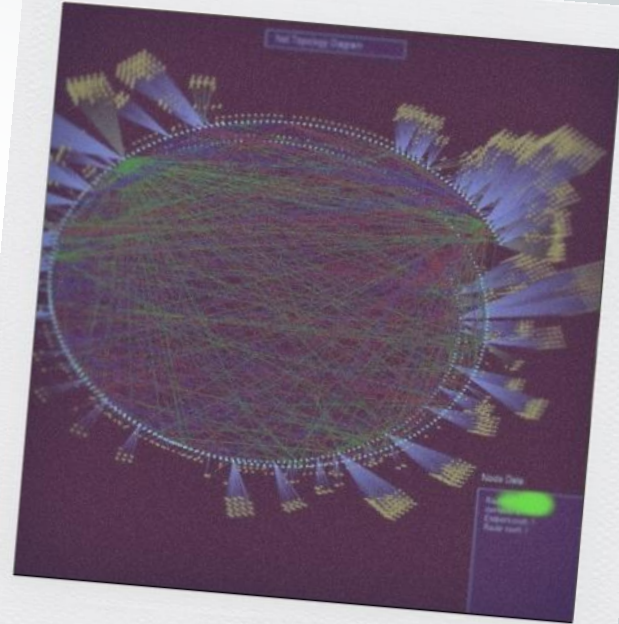
# The risk for ISPs/Data Centre Operators

- Ever Changing IT Environment
  - Virtualization, Cloud, IoT
    - *You are not sure what you have in your network*
- Tight man power
  - Growth of IT team is far behind growth of device
- Silo Pieces of component
  - Security, Monitoring and Reporting solution work separately

# The risk for ISPs/Data Centre Operators



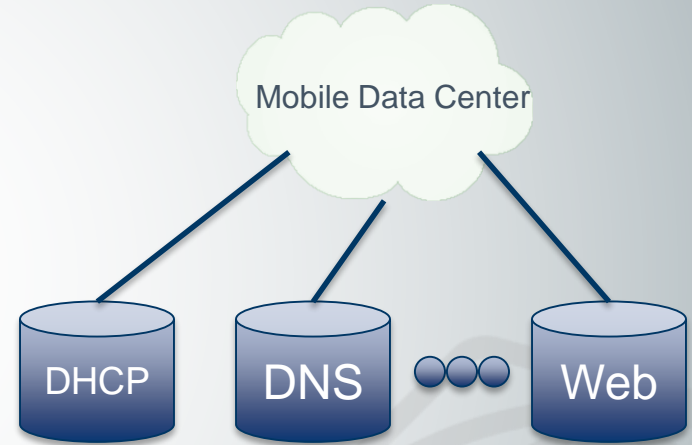
Network Jan 2014



Network June 2014

# The risk for ISPs/Data Centre Operators

- Contains essential support functions for Mobile Network to operate
  - DHCP
  - DNS
  - Web portals
  - Value-add custom services
  - ...
- Things like HLR (Home Location Register) logically reside in another place but generally physically reside in MDC

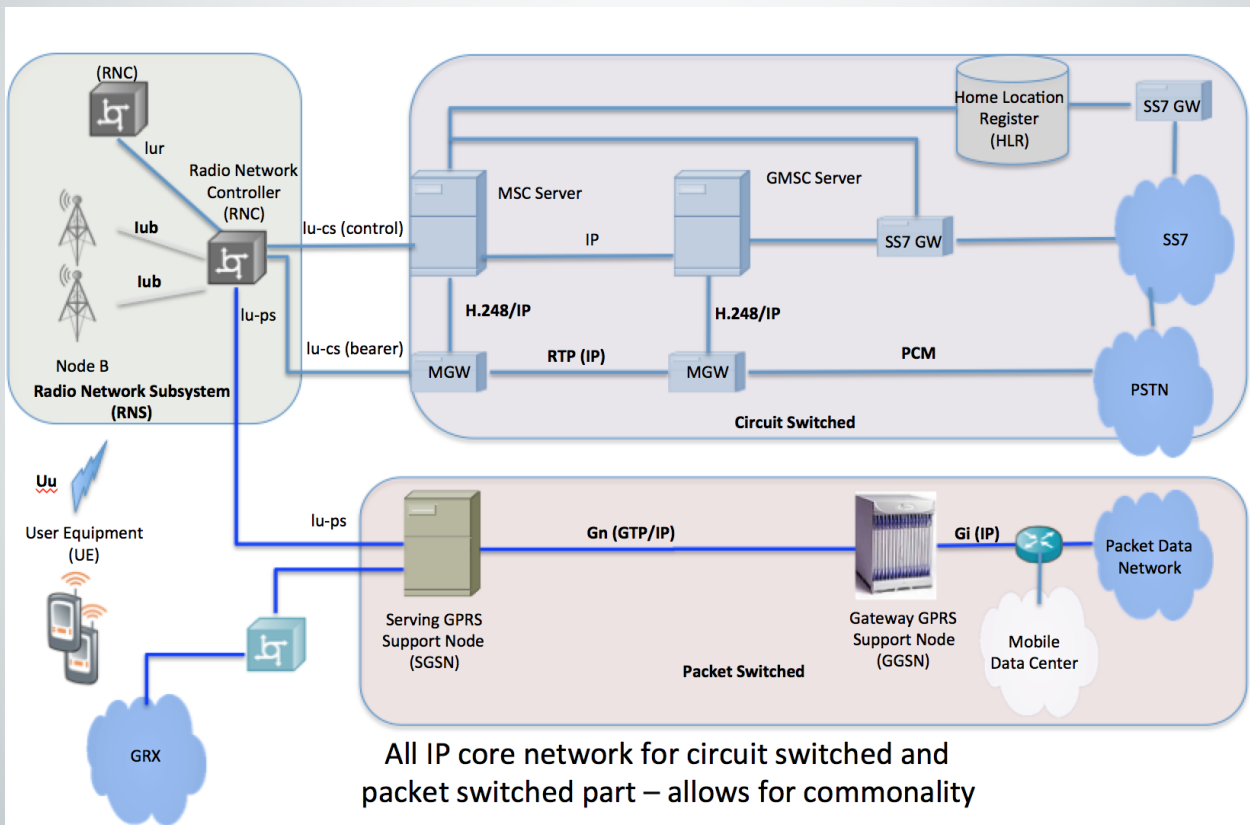


# The risk for ISPs/Data Centre Operators

---

- Critical parts of infrastructure within network now use commodity components
  - Which have vulnerabilities
- More and more device use IP, especially in 4G
  - Possibility to access by others

# What would you attack?



What would you attack?

---

How to measure our ***RISK***?



# THE RATE AT WHICH VULNERABILITIES EMERGE

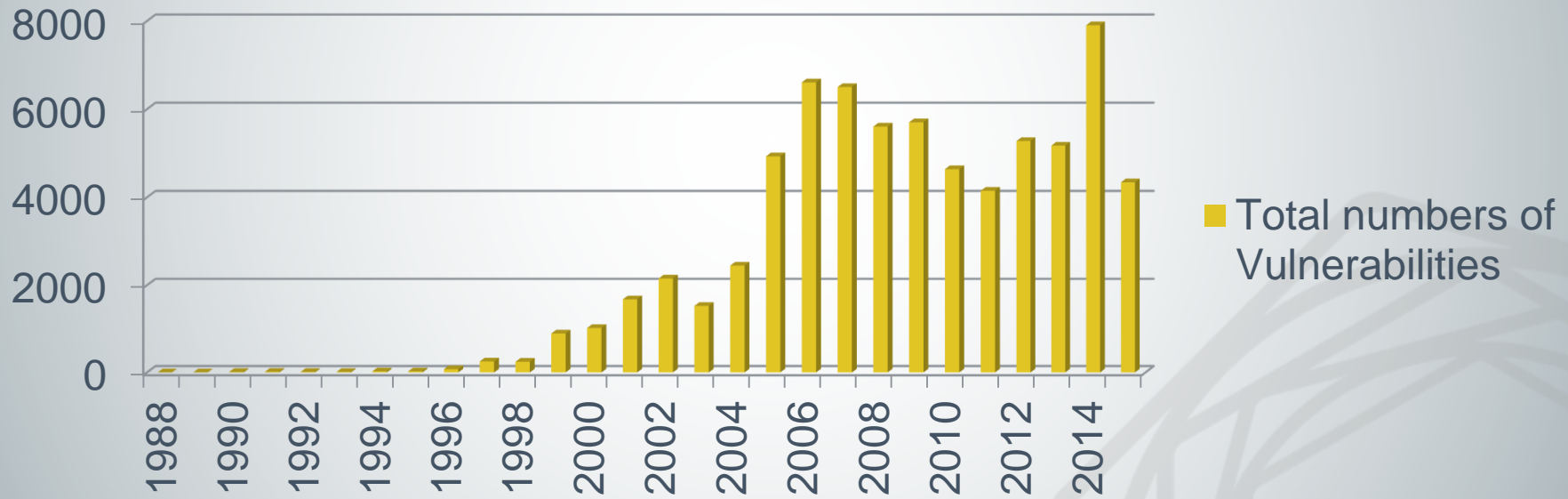
---





# The Rate at which Vulnerabilities Emerge

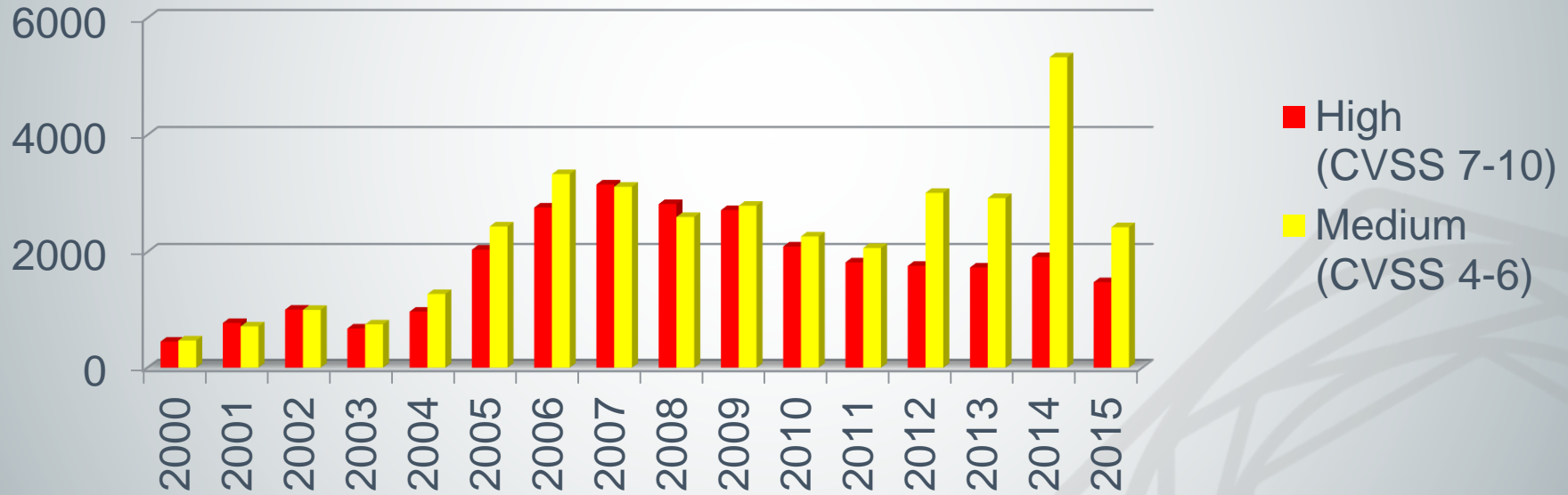
**Total numbers of Vulnerabilities**



Source: NIST Vulnerabilities Database

# The Rate at which Vulnerabilities Emerge

*Since 2005, we have around 2000 High Risk vulnerabilities published every year, it's about 5-6 vulnerabilities per day.*



Source: NIST Vulnerabilities Database

# **SOME EXAMPLES OF ISP COMPROMISE AND THE IMPACT**

---



# Examples of ISP Compromise and The Impact

- 2014-Dec, TalkTalk (UK Broadband provider)
  - 4 Millions customer data expose, many customer receive fraud call after.
- 2015-May, Telstra Pacnet (Telco)
  - Customer data expose, Pacnet inform customers that they are hacked.
- 2015-Jun, Westnet (Australia Telco)
  - Customer data leak (hacker reselling their data), password reset.
- 2015-Aug, ICAAN
  - End user information, global password reset.

# **THE CONTINUOUS VULNERABILITY MANAGEMENT METHODOLOGY**

---



# Assurance with Tenable

## COMPLETE VISIBILITY

Know Your Network



### **Breadth of Sensors**

Collect & integrate critical  
data across the enterprise

# Active Scanning





# Active Scanning



# Active Scanning

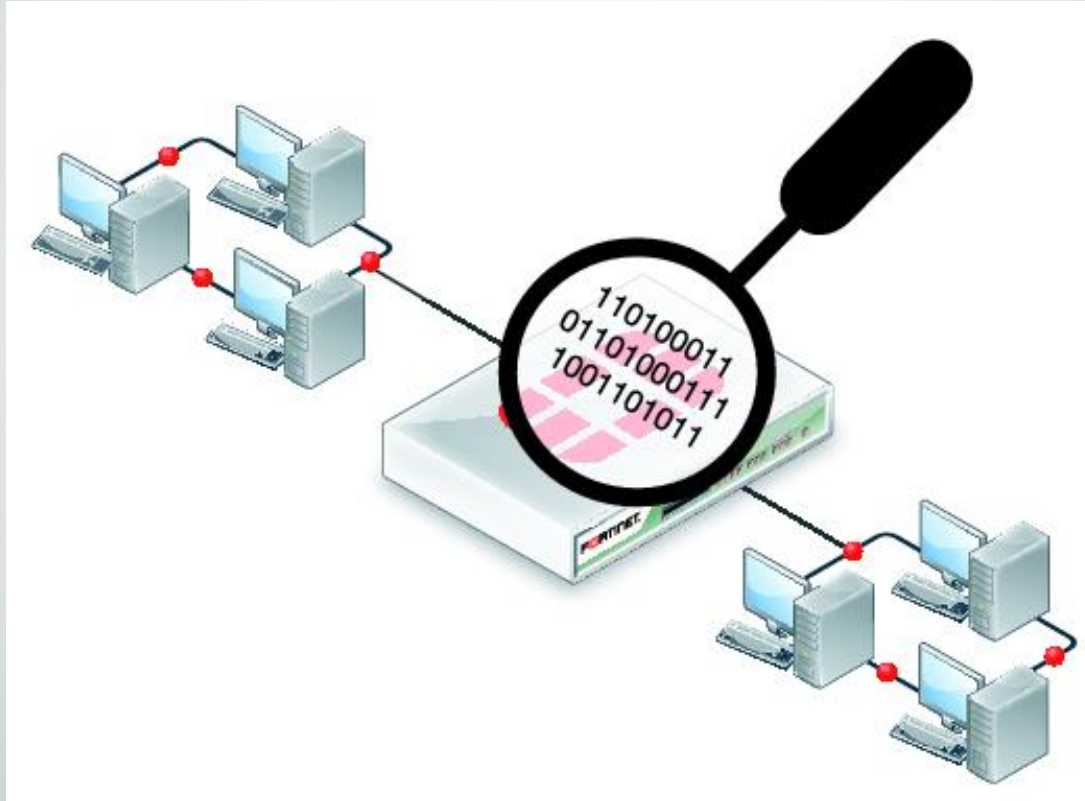
- May miss transient devices, if they are disconnected
- Will miss devices outside the specified address range
- Highly Accurate
- Grossly Inefficient

# Agents

- Mobile workforce
- Lower bandwidth sites
- Super small and light weight
- Highly Accurate
- Require Agent Install



# Passive Network Monitoring



# Passive Network Monitoring



# Passive Network Monitoring

## Continuously Monitors Network Traffic

- Discovers transient assets
- Uses fingerprinting to determine OS & version
- Discovers active ports, protocols, and services
- Discovers client applications
- Always on
- Less Accurate



# Intelligent Connectors

Spraying packets is no longer the only way to find hosts

- Clouds
- Active Directory
- Patch management systems
- IP management solutions
- Etc.





# Host Data

- Cyber Hygiene
- Scanning is still set at some periodicity
- Rich in Details
- Lot's of information



# Five-Fingers Approach

---

1. Active Scan
2. Agents
3. Passive Vulnerability Scan
4. Intelligent Connectors
5. Host Data

# Assurance with Tenable

## COMPLETE VISIBILITY

Know Your Network



### **Breadth of Sensors**

Collect & integrate critical data across the enterprise

## BETTER CONTEXT

Know What To Do



### **Measure and Report**

Prioritize security issues based on actionable intelligence

## TOTAL ASSURANCE

Know You're Secure



### **Continuous Monitoring**

Real-time, advanced analysis

# **BENEFITS / CONCLUSION**

---



# Benefits

- Collect Data from ***Different Sources***
- Transform ***Data*** to ***Information***
- Understand ***what you have*** (hardware / software) in your IT Infrastructure
- Combine ***Context*** and ***Business*** needs to risk management
- ***Continuously*** Monitor your IT infrastructure

# Customer Case Study

- Service Provider in APAC
- Holder of 4G License
- Roll out more then 800 cities



# The Problem Space

- Security is forefront in the mind of this customer
  - Vulnerability management and continuous monitoring considered from initial build-out
- How to protect...
  - Core infrastructure?
  - Offered services running over that infrastructure?
- Huge operation
  - More than 300,000 IP addresses in more than 800 cities
  - Complex environment consisting of BSS, Wireless equipment, custom software, network equipment, servers...
  - Total of 60,000 **physical** Servers (growing)



# Vulnerability Management as internal SaaS

- Establish compliance standards and targets
- Define operational groups (16 total)
  - Assign assets to each group
    - Technical infrastructure is “flat”
- Assign a SecurityCenter “portal” to each group
  - Each group manages their own assets using SecurityCenter
    - Pre-deployment, testing, deployed services all covered
  - Overall compliance management/security organization ensures each group meeting its objectives

# Customer Objectives

---

- Reduce and maintain vulnerabilities at an ***acceptable level***
- ***Real-time detection*** of vulnerabilities and misconfigurations
- Maintain a “***report card***” for each of the 16 organizations
- Detect ***early indications*** of compromise
- Detect inbound ***suspicious or malicious activities***
- ***Augment and supplement services*** provided by SIEM

# Assurance Report Cards

+ Add

Options ▾

- CCC 1: Maintain an Inventory of Software and Hardware

x x x x ✓ ✓

◀
- CCC 2: Remove vulnerabilities and misconfigurations

x x x x x

◀
- CCC 3: Deploy a secure network

x ✓ ✓ ✓ x x

◀
- CCC 4: Authorize Users

x x x x x

◀
- CCC 5: Search for malware and intruders.

✓ ✓ x x ✓ ✓

◀



CCC 1: Maintain an Inventory of Software and Hardware

x x x x x ✓ ✓ ◀









CCC 2: Remove vulnerabilities and misconfigurations

x x x x x ◀

**CCC 3: Deploy a secure network**

Last Evaluated 21 hours ago ↻

-  1. Less than 5% of systems accepting external connections have an exploitable vulnerability. 3 / 8
-  2. Less than 5% of Security Devices (Firewall, VPN, and Load Balancers) have a critical vulnerability. 0 / 0
-  3. Less than 5% of Systems with VPN access have a exploitable vulnerabilities older than 30 days. 0 / 1
-  4. Less than 10% of systems utilize insecure protocols external to the organization. 5 / 22776
-  5. Greater than 90% of firewalls have their logs centrally stored. 0 / 0
-  6. Greater than 95% of internet facing systems have centralized log collection enabled. 6 / 8



CCC 4: Authorize Users

x x x x x ◀









CCC 5: Search for malware and intruders.

✓ ✓ x x ✓ ✓ ◀



### CCC 3: Deploy a secure network

Last Evaluated 21 hours ago 

	1. Less than 5% of systems accepting external connections have an exploitable vulnerability.	3 / 8
	2. Less than 5% of Security Devices (Firewall, VPN, and Load Balancers) have a critical vulnerability.	0 / 0
	3. Less than 5% of Systems with VPN access have a exploitable vulnerabilities older than 30 days.	0 / 1
	4. Less than 10% of systems utilize insecure protocols external to the organization.	5 / 22776
	5. Greater than 90% of firewalls have their logs centrally stored.	0 / 0
	6. Greater than 95% of internet facing systems have centralized log collection enabled.	6 / 8

## Indicators - Botnet Activity

Bot List	Inbound Netstat	Outbound Netstat	DNS Bot Config	Bot URLs
Bot Attacks	Inbound Traffic	Outbound Traffic	Bot Auth	Bot Anomalies

## Indicators - Continuous Events

IDS	Scanning	Malware	Botnet	DOS
Sys Errors	Web Error	Win Error	High CPU	DNS Errors

## Indicators - Malicious Process Monitoring

Malicious (Scan)	Unwanted	Custom Hash	Indicator	Multi Crashes
Process Spike	Virus Spike	Error Spike	Change Spike	FIM Spike
New EXE Spike	Unique Unix	Unique Win	Malicious (LCE)	Bad AutoRuns

## Indicators - Access Control Anomalies

Firewall Spike	Auth Spike	Auth Fail Spike	Access Spike	Denial Spike
----------------	------------	-----------------	--------------	--------------

## Indicators - Intrusion Detection Events

Targeted	Host Scan	Net Sweep	Web Scan	Web Sweep
Auth Sweep	Auth Guessing	Auth Guessed	Worm Activity	IDS Spike
Scan Spike	DNS Tunnel	Web Tunnel	EXE Serve	USER Auth

## Indicators - Network Anomalies and Suspicious Activity

DNS Spike	SSL Spike	PVS Spike	Network Spike	Netflow Spike
File Spike	Web Spike	404+ Spike	Inbound Spike	Outbound Spike
SSH 30m+	VNC 30m+	RDP 30m+	Internal Spike	Connect Spike

## Indicators - Exploitable Internet Services

Services	FTP	SSH	HTTP	HTTPS	SMB
Ports	1-200	201-500	501-1024	1025-5000	5000+

## Indicators - Suspicious Proxies, Relays and SPAM

Proxy	SSH Proxy	VNC Proxy	RDP Proxy	Bot Proxy
SMTP Proxy	SMTP Relay	SPAM Server	Crowd Surge	

## Filters



## Normalized Event ✕

=  
Threatlist\_Inbound\_Connectio  
n\_HTTPS

## Type ✕

threatlist

## Timeframe ✕

Between Jun 25, 2015 11:55  
and Jul 20, 2015 11:55 / 25  
Days

## Address

All

## Syslog Text

All

Type Summary ▸ Normalized Event Summary ▸ List of Events ▸

Total Results: 692

Raw Syslog Events ▾

Time	Type ▲	Se...	Message	
Jun 29, 2015 06:15	threatlist	TASL	Threatlist_Inbound_Connection_HTTPS src - 10[REDACTED]:2620 dst - 172.16.132.2:443 , supplied by Bot , the event was triggered by a TNM-TCP_Session_Short event	—
Jun 29, 2015 06:15	threatlist	TASL	Threatlist_Inbound_Connection_HTTPS src - 10[REDACTED]:1906 dst - 17	+
Jun 29, 2015 06:16	threatlist	TASL	Threatlist_Inbound_Connection_HTTPS src - 10[REDACTED]:64566 dst - 1	+
Jun 29, 2015 06:16	threatlist	TASL	Threatlist_Inbound_Connection_HTTPS src - 10[REDACTED]:58199 dst - 1	+
Jun 29, 2015 06:17	threatlist	TASL	Threatlist_Inbound_Connection_HTTPS src - 10[REDACTED]:31159 dst - 1	+
Jun 29, 2015 06:17	threatlist	TASL	Threatlist_Inbound_Connection_HTTPS src - 10[REDACTED]:14246 dst - 1	+
Jun 29, 2015 06:18	threatlist	TASL	Threatlist_Inbound_Connection_HTTPS src - 10[REDACTED]:19326 dst - 1	+
Jun 29, 2015 06:18	threatlist	TASL	Threatlist_Inbound_Connection_HTTPS src - 10[REDACTED]:14788 dst - 1	+
Jun 29, 2015 06:19	threatlist	TASL	Threatlist_Inbound_Connection_HTTPS src - 10[REDACTED]:15688 dst - 1	+
Jun 29, 2015 06:19	threatlist	TASL	Threatlist_Inbound_Connection_HTTPS src - 10[REDACTED]:17221 dst - 1	+



# Event Analysis

Options ▾



Type Summary ▸

Normalized Event Summary ▾

Jump to Raw Syslog Events

Total Results: 2

2

Event ▲	Count	Trend Data	
Threatlist_Inbound_Connection_High_Port	1		⚙️ ▾
Threatlist_Inbound_Connection_HTTPS	692		⚙️ ▾

# Conclusion

- Ever Changing IT Environment
  - Inventory ***all*** hardware and software is ***possible*** now with Tenable's 5 fingers approach
- Critical parts of infrastructure within network now use commodity components
  - Periodic scan is not enough to ***understand your risk***
  - Implement ***different method*** (active, passive, host data) to ***identify vulnerabilities***

# Conclusion

- More and more device use IP, especially in 4G
  - ***Continuously Monitor*** the ***network, protocols*** and communications pattern should be stable and not change much. Threads can be identify by ***pattern change***.
- Tight man power, Silo Pieces of component
  - Combine Context and Business requirement to define your own ***Security Metrics***
  - Single console to monitor your security metrics
  - Continuously Monitor the ***Metrics*** to **Enhance Security Posture**



**tenable**<sup>®</sup>  
network security