



Inside the Perimeter

6 Steps to Improve Your Security Monitoring



Chris Fry, CCSP

Martin G. Nystrom, CISSP-ISSAP

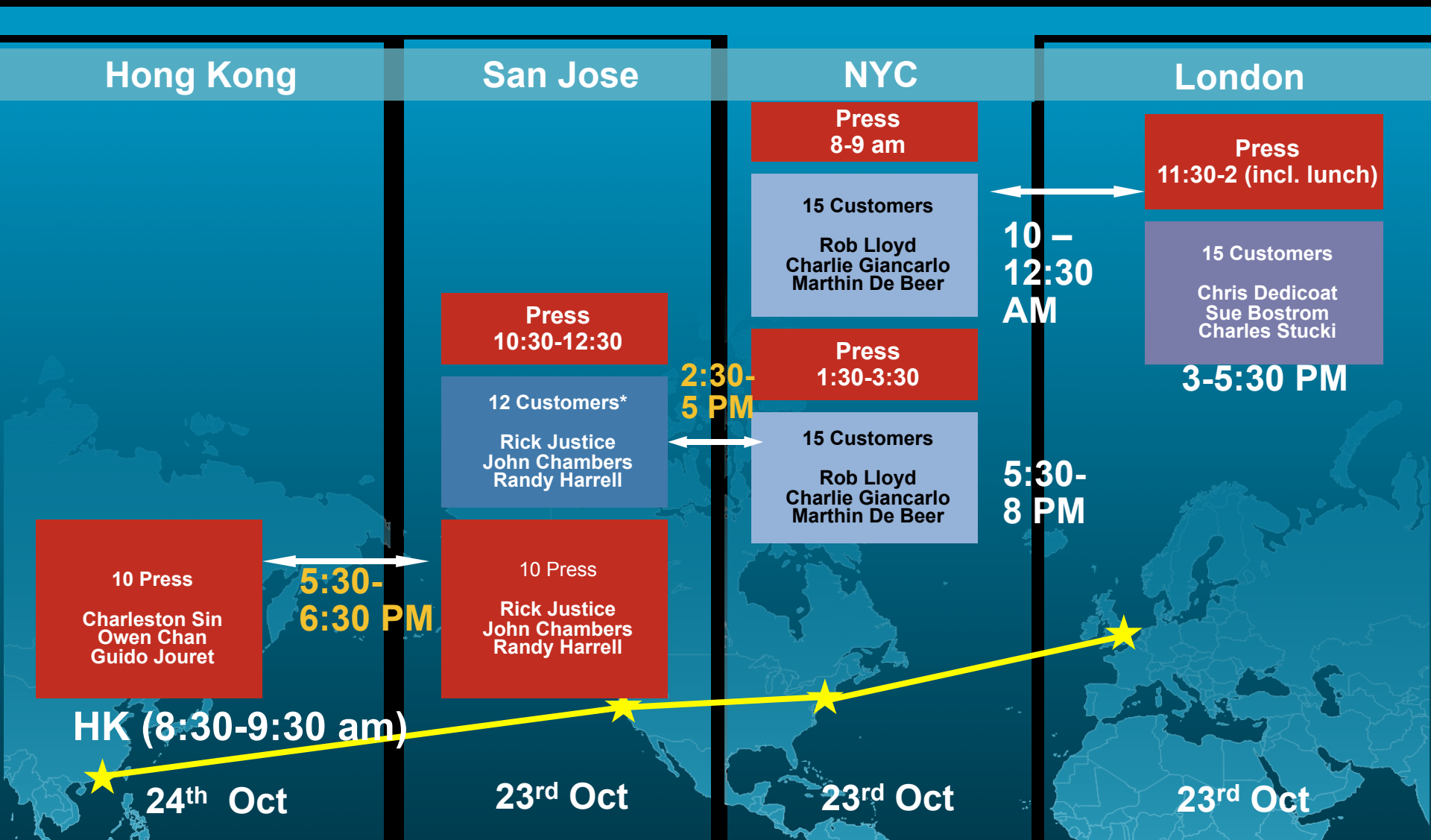
Cisco CSIRT

Cisco TelePresence

Next-generation IP video conferencing

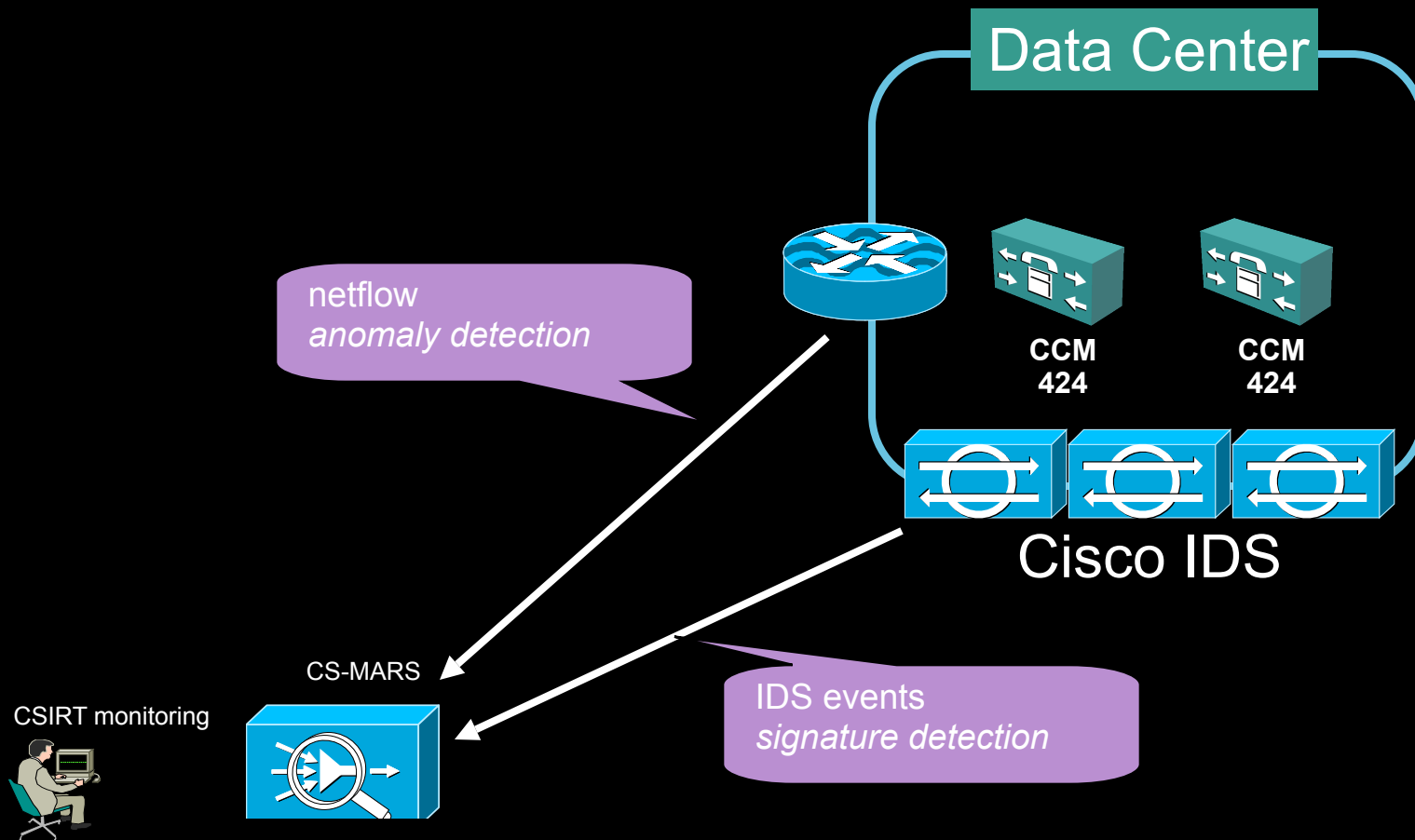


TelePresence Public Launch Across Theatres



Monitoring Architecture

Cisco IDS, Netflow, and CS-MARS











False Positive Traffic Example: *SSH sync between CM's*





Report Results (List): TelePresence Event Monitoring Oct 23, 2006 2:02:47 PM PDT - Oct 23, 2006 3:02:47 PM PDT

| Name | Schedule | Format | Recipients | Query | Description | Status | Submitted | Time Range |
|-------------------------------|------------|------------|-------------------------|---|--|--------|-----------|--------------------------------|
| TelePresence Event Monitoring | Every hour | Total View | Local: MAILER, CSOCNone | Src: [171.68.196.0 / 255.255.255.0] US-West - SJC-K Data Center Call Managers Cluster Servers, [171.70.147.90 / 255.255.255.128] US-West - SJC12 Call Managers (SJC12-CM4-PROD1) OR Dest: [171.70.147.90 / 255.255.255.128] US-West - SJC12 Call Managers (SJC12-CM4-PROD1), [171.68.196.0 / 255.255.255.0] US-West - SJC-K Data Center Call Manager Cluster Servers Query Type: Sessions ranked by Time Time: 0d-1h:00m | False Positive: normal sync traffic | | | |
| | | | | | | | | Oct 23, 2006 3:02:47 PM PDT |

**False Positive:
normal sync traffic
between call
managers**

Report type: Sessions ranked by Time, 0d-1h:00m [Edit](#) [Clear](#)

| Open (| Source IP | Destination IP | managers | | | | |) Close | Operation |
|---|--|--|----------|-----|-----|-----|-----|---|-----------|
|   | [171.68.196.0 / 255.255.255.0] US-West - SJC-K Data Center Call Manager Cluster Servers, [171.70.147.90 / 255.255.255.128] US-West - SJC12 Call Managers (SJC12-CM4-PROD1) | ANY | ANY | ANY | ANY | ANY | ANY |   | OR |
|   | ANY | [171.70.147.90 / 255.255.255.128] US-West - SJC12 Call Managers (SJC12-CM4-PROD1), [171.68.196.0 / 255.255.255.0] US-West - SJC-K Data Center Call Manager Cluster Servers | ANY | ANY | ANY | ANY | ANY |   | None |

| Session / Incident ID | Events | Source IP/Port | | Destination IP/Port | | Protocol | Time | Reporting Devices | Path / Mitigation | Tune |
|---|---|----------------|-------|---------------------|----|----------|--|---|---|-----------|
| S:141757560997, I:141747530252 I:141747530254 | Multiple Rapid SSH Connections Context data TCP SYN Host Sweep On Same Dest Port SNMP Protocol Violation | 171.68.196.101 | 49638 | 171.70.147.90 | 22 | TCP | Oct 23, 2006 1:56:36 PM PDT - Oct 23, 2006 2:14:11 PM PDT | sjck-dc-nms-4, sjck-dc-nms-1, sjck-dc-nms-3, sjc12-dc2-nms-2 |   | False Pos |
| S:141757560997, I:141747530252 I:141747530254 | Multiple Rapid SSH Connections Context data TCP SYN Host Sweep On Same Dest Port SNMP Protocol Violation | 171.68.196.101 | 49638 | 171.70.147.90 | 22 | TCP | Oct 23, 2006 1:56:36 PM PDT - Oct 23, 2006 2:14:11 PM PDT | sjck-dc-nms-4, sjck-dc-nms-1, sjck-dc-nms-3, sjc12-dc2-nms-2 |   | False Pos |

Security Event Example: *Infected host attacking call managers*

| Name | Schedule | Format | Recipients | Query | Description | Status |
|-------------------------------|------------|------------|-------------------------|--|---|------------------------------|
| TelePresence Event Monitoring | Every hour | Total View | Local: MAILER, CSOCNone | Src: [171.68.196.0 / 255.255.255.0] US-West - SJC-K Data Center Call Manager Cluster Servers, [171.70.147.90 / 255.255.255.128] US-West - SJC12 Call Managers (SJC12-CM4-PROD1) OR Dest: [171.70.147.90 / 255.255.255.128] US-West - SJC12 Call Managers (SJC12-CM4-PROD1), [171.68.196.0 / 255.255.255.0] US-West - SJC-K Data Center Call Manager Cluster Servers Query Type: Sessions ranked by Time Time: 0d-1h:00m | Monitor for all events sourced from or terminating into the Telepresence CallManager clusters. For use on October 23rd for targeted monitoring. | Finished: 0 2006 11:0 AM PDT |

**IDS and MARS
detecting hosts
attacking call
managers**

Report type: Sessions ranked by Time, 0d-1h:00m

| Open (| Source IP | Destination | Service | Events | Device | Reported User | K |
|--------|--|--|---------|--------|--------|---------------|----|
| | [171.68.196.0 / 255.255.255.0] US-West - SJC-K Data Center Call Manager Cluster Servers, [171.70.147.90 / 255.255.255.128] US-West - SJC12 Call Managers (SJC12-CM4-PROD1) | ANY | ANY | ANY | ANY | ANY | AF |
| | ANY | [171.70.147.90 / 255.255.255.128] US-West - SJC12 Call Managers (SJC12-CM4-PROD1), [171.68.196.0 / 255.255.255.0] US-West - SJC-K Data Center Call Manager Cluster Servers | ANY | ANY | ANY | ANY | AF |

| Session / Incident ID | Events | Source IP/Port | Destination IP/Port | Protocol | Time | Reporting Devices |
|-----------------------|---|---------------------|---------------------|----------|------------------------------|-------------------|
| S:141616106043 | Windows RPC DCOM Overflow | 171.69.126.28 3220 | 171.68.196.70 135 | TCP | Oct 23, 2006 10:22:17 AM PDT | sjck-dc-nms-1 |
| S:141615830105 | Windows RPC DCOM Overflow , Context data | 171.69.126.28 3220 | 171.68.196.70 135 | TCP | Oct 23, 2006 10:22:00 AM PDT | sjck-dc-nms-1 |
| S:141615830122 | Windows SMB/RPC NoOp Sled , Context data | 171.69.126.28 3220 | 171.68.196.70 135 | TCP | Oct 23, 2006 10:22:00 AM PDT | sjck-dc-nms-1 |
| S:141615830124 | Windows SMB/RPC NoOp Sled , Context data | 171.69.126.28 3221 | 171.68.196.71 135 | TCP | Oct 23, 2006 10:22:00 AM PDT | sjck-dc-nms-1 |
| S:141615830126 | Windows SMB/RPC NoOp Sled , Context data | 171.69.126.28 3228 | 171.68.196.78 135 | TCP | Oct 23, 2006 10:22:00 AM PDT | sjck-dc-nms-1 |
| S:141615830117 | Nachi Worm Spread and DoS via ICMP Ping | 171.69.126.28 0 | 171.68.196.2 0 | ICMP | Oct 23, 2006 10:21:59 AM PDT | sjck-dc-nms-1 |

Attacking host was blackholed and submitted for remediation

6 steps to improve your security monitoring

- 
- 1. Know your policy**
 - 2. Know the network**
 - 3. Select targets**
 - 4. Choose event sources**
 - 5. Feed and tune**
 - 6. Troubleshoot**

What We Assume About Our Audience

- You've got an **incident response** team
- You have experience **deploying tools** and **monitoring**
- Focus on discussing *deploying* monitoring solutions





**Step 1.
Build and
understand
your policy**

Monitor Against Defined Policies

- Which policies to monitor?
 - Be concrete, precise
 - Which will management enforce?

- Types of policies

Compliance with regulations or standards

SOX – monitor financial apps and databases

HIPAA – monitor healthcare apps and databases

ISO 17799 - best practices for information security

Employee policies

Rogue devices – laptops, wireless, DC devices, honeypots, etc.

Employees using shared accounts

Hardened DMZ devices – services running that should not be?

Direct login with privileged accounts (root, DBA, etc.)

Tunneled traffic – P2P, etc.



Policy Monitoring Examples

- Policy: **COBIT DS9.4: Configuration Control**

Monitor changes to network devices, reconcile against approved change lists

- Policy: **No direct privileged logins**

Monitor IDS, SSH logs for successful *root* logins

- Policy: Use **strong passwords**

Vulnerability scan for routers with *cisco/cisco* credentials

- Policy: **No internet access from production servers**


Monitor for accepted connections to Internet initiated from servers

- Policy: **No protocol tunneling**

Monitor IDS alerts for protocols tunneled over DNS to/from non-DNS servers

Example: FTP Root Login

```
evIdsAlert:  eventId="1173129985693574851"  severity="low"  vendor="Cisco"
  originator:
    hostId:  rcdn4-dmz-nms-1
    appName:  sensorApp
    appInstanceId:  421
  time:  Mar 22 2007 18:14:39 EDT (1173129985693574851)  timeZone="UTC"
  signature:  version="S31"  description="Successful Login via FTP"  id="3171"
    subsigId:  1
    sigDetails:  USER administrator
    marsCategory:  Info/SuccessfulLogin/FTP
  interfaceGroup:  vs0
  vlan:  0
  participants:
    attacker:
      addr:  163.180.17.91  locality="OUT"
      port:  1387
    target:
      addr:  12.19.88.226  locality="IN"
      port:  21
      os:  idSource="unknown"  relevance="unknown"  type="unknown"
  summary:  2  final="true"  initialAlert="1173129985693574773"  summaryType="Regular"
  alertDetails:  Regular Summary: 2 events this interval ;
  riskRatingValue:  37  targetValueRating="medium"
  threatRatingValue:  37
  interface:  ge0_0
  protocol:  tcp
```



Example: SSH root login message

A red speech bubble with a white border, containing the text "Caught direct root login via syslog". It points towards the log message.

Caught direct root
login via syslog

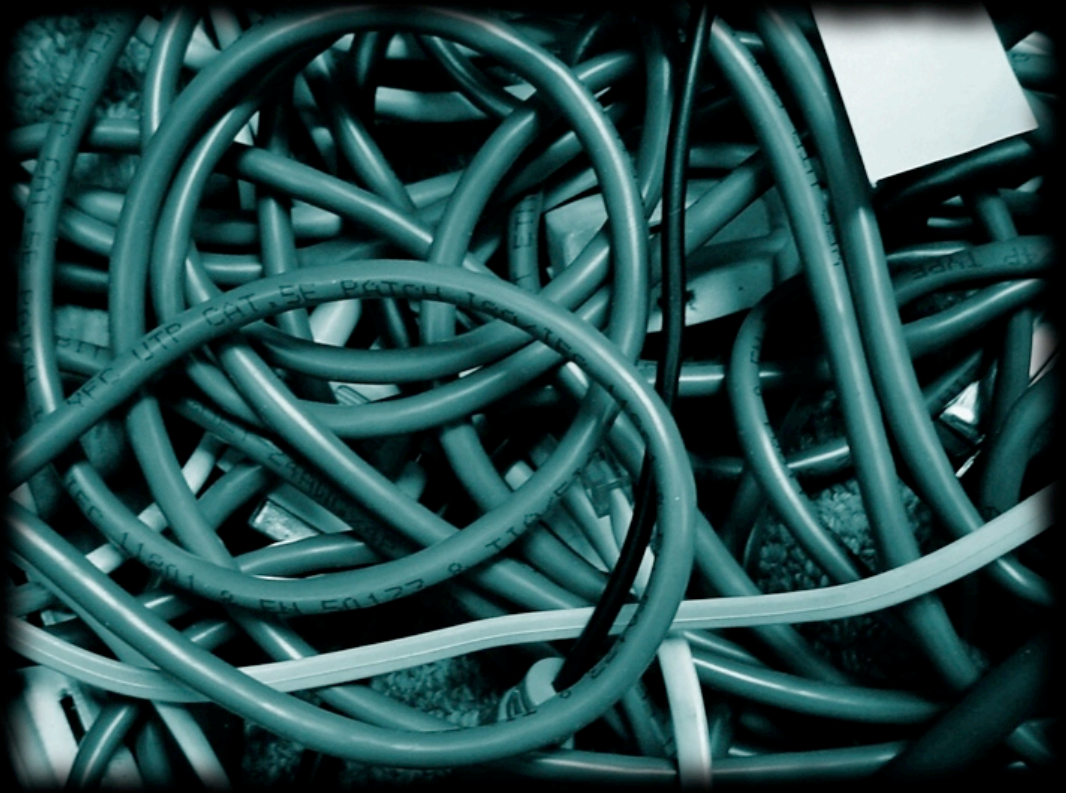
```
Mar 28 16:19:01 xianshield sshd[198]:  
session opened for user root by (uid=0)
```

Step 2: Know Your Network



Do You Have a **Self Defeating** Network?

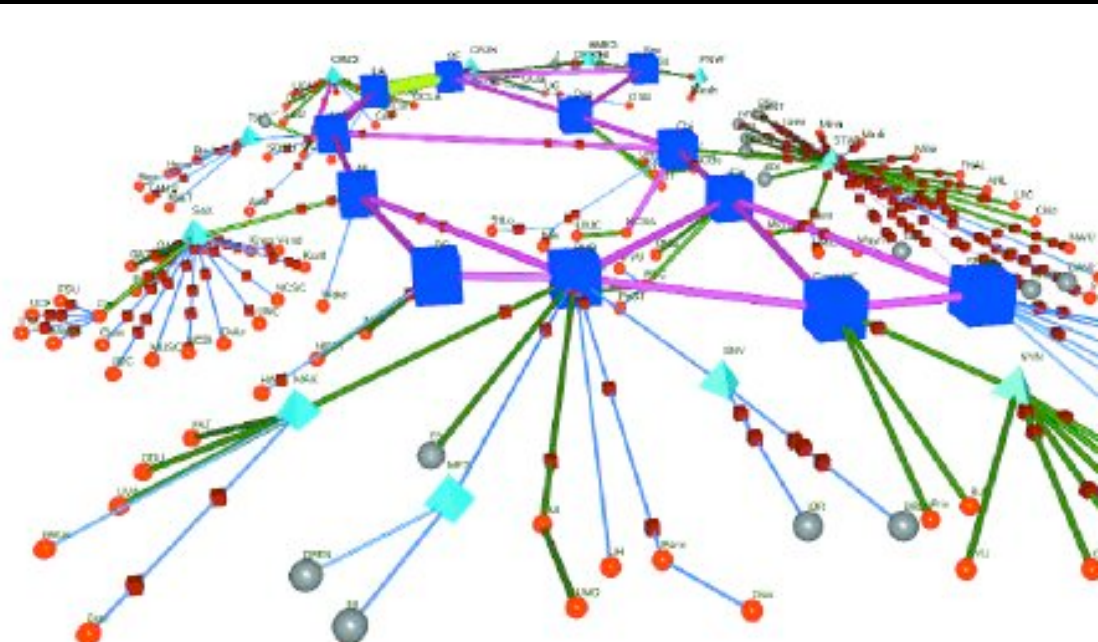
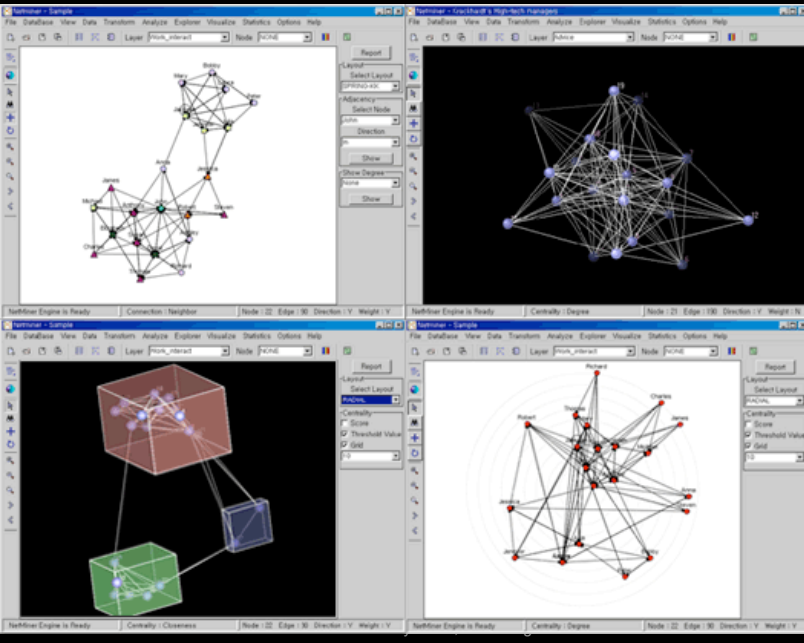
- Unknown
- Unmonitored
- Uncontrolled
- Unmanned
- Trusted



Source: Richard Bejtlich

What Is Meant by 'Telemetry'?

Te·lem·e·try — a technology that allows the **remote measurement and reporting of information of interest** to the system designer or operator. The word is derived from Greek roots *tele* = remote, and *metron* = measure



Network Telemetry - What's it Do For Me?

- Historically used for capacity planning
- Detects attacks
 - With analysis tools, can detect anomalies
- Supports investigations
 - Tools can collect, trend, and correlate activity
- Well supported
 - Arbor PeakFlow
 - CS-MARS
 - NetQoS
 - OSU FlowTools
- Simple to understand



Network Telemetry — Time Synchronization



- Without it, can't correlate different sources
- Enable Network Time Protocol (NTP) everywhere
 - supported by routers, switches, firewalls, hosts, and other network-attached devices
- Use UTC for time zones

What is NetFlow?

- NetFlow is a form of **telemetry** pushed from the network devices.
- Netflow is best used in combination with other technologies: IPS, vulnerability scanners, and full traffic capture.

Traffic capture is like a **wiretap**

NetFlow is like a **phone bill**

- We can learn a lot from studying the network phone bill!

Who's talking to **whom?** And **when?**

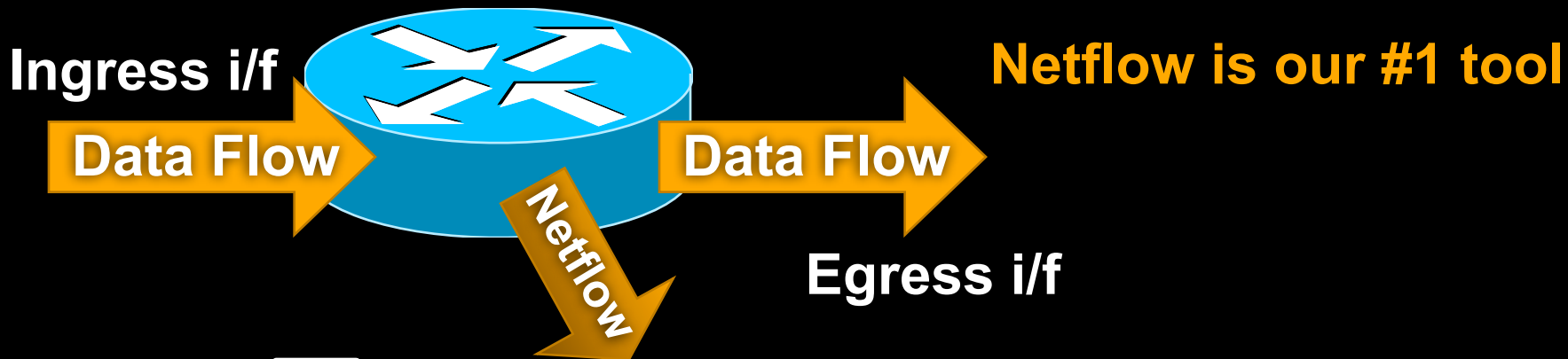
Over **what protocols & ports?**

How much data was transferred?

At **what speed?**

For **what duration?**

Netflow

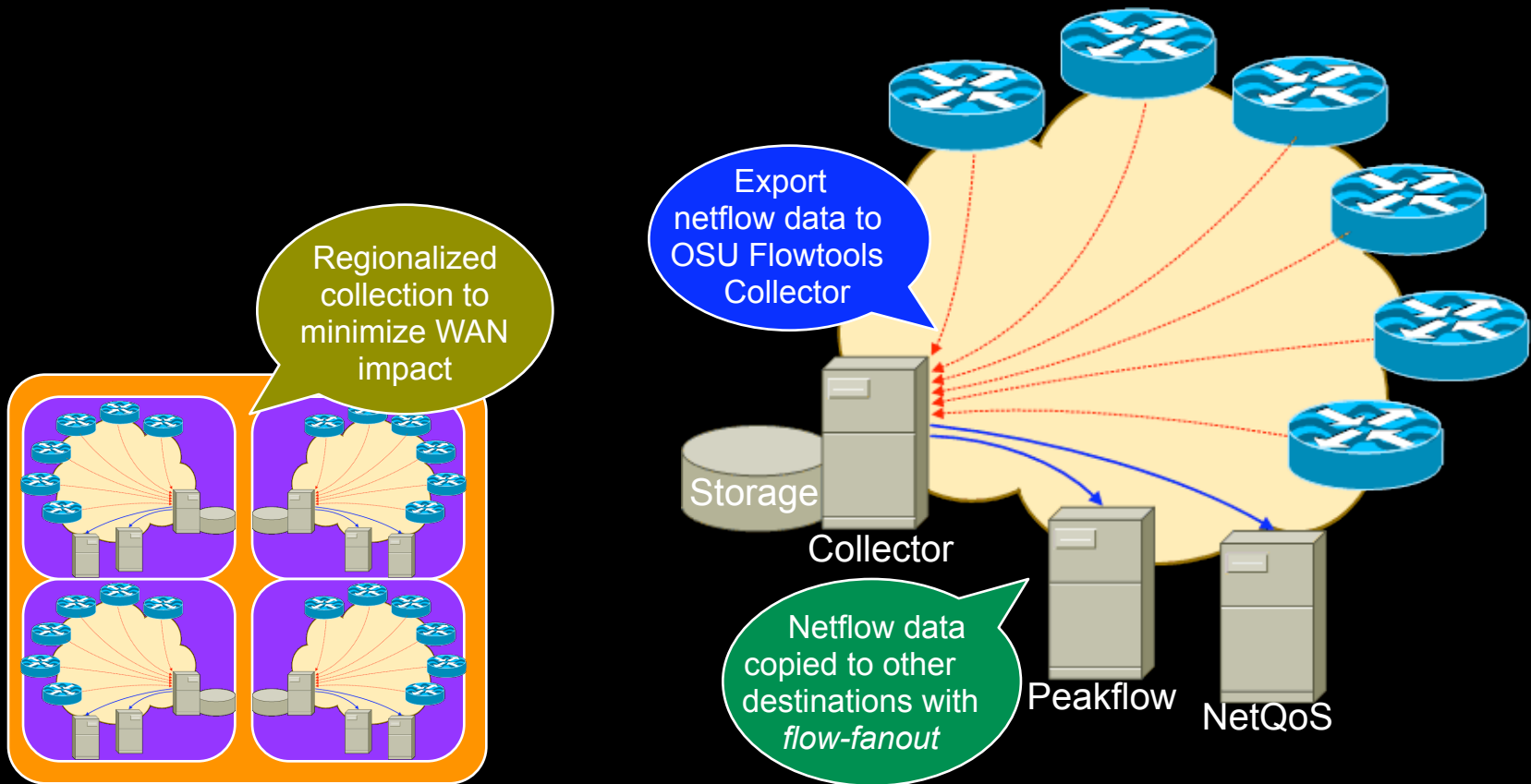


| | | | |
|-------------------------|--|---|----------------------------|
| <u>Usage</u> | <ul style="list-style-type: none"> • Packet Count • Byte Count | <ul style="list-style-type: none"> • Source IP Address • Destination IP Address | <u>From/To</u> |
| <u>Time of Day</u> | <ul style="list-style-type: none"> • Start sysUpTime • End sysUpTime | <ul style="list-style-type: none"> • Source TCP/UDP Port • Destination TCP/UDP Port | <u>Application</u> |
| <u>Port Utilization</u> | <ul style="list-style-type: none"> • Input ifIndex • Output ifIndex | <ul style="list-style-type: none"> • Next Hop Address • Source AS Number • Dest. AS Number | <u>Routing and Peering</u> |
| <u>QoS</u> | <ul style="list-style-type: none"> • Type of Service • TCP Flags • Protocol | <ul style="list-style-type: none"> • Source Prefix Mask • Dest. Prefix Mask | |

Netflow Setup

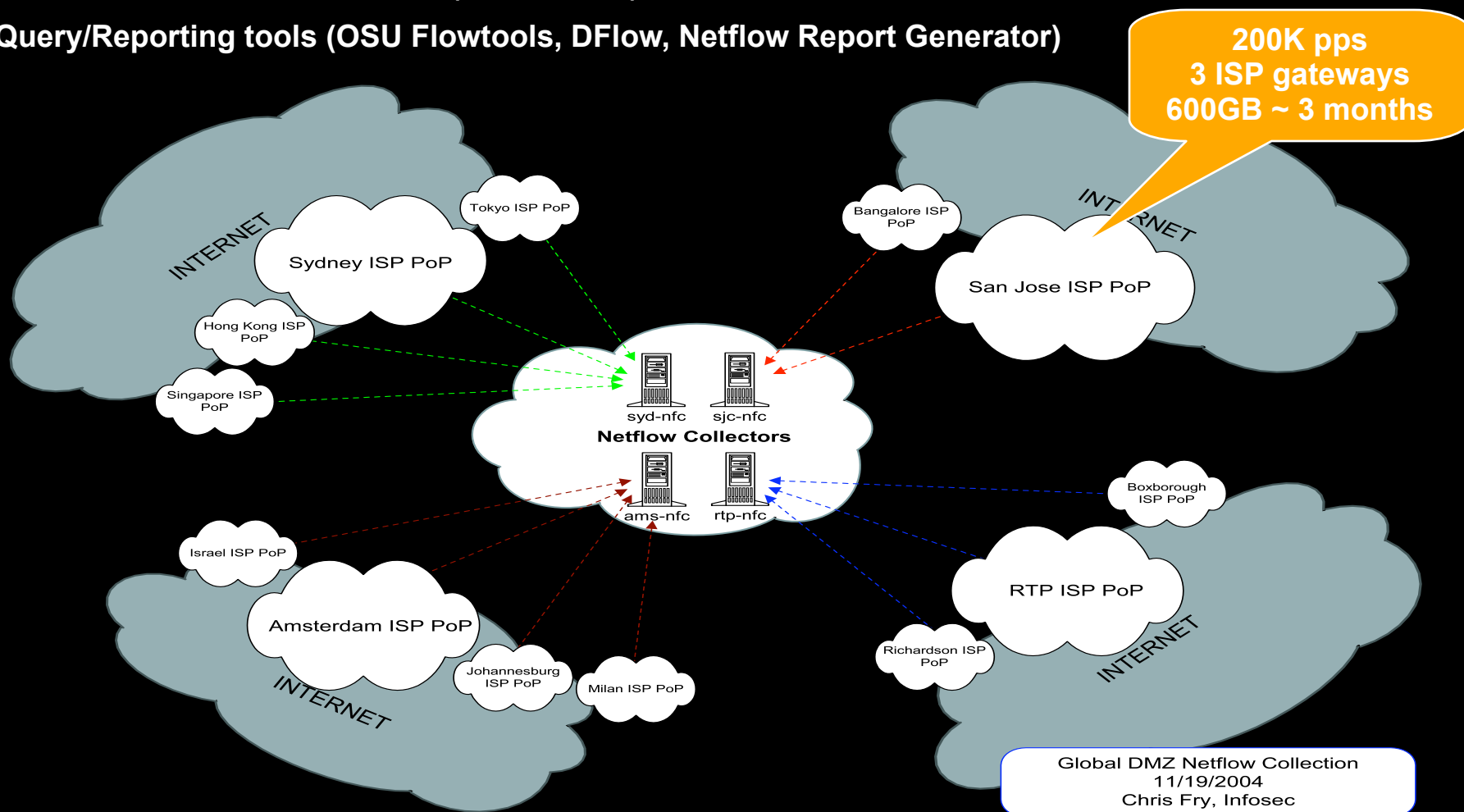
- Don't have a copy of netflow data b/c IT won't share?

Many products have the ability to copy flow data off to other destinations



NetFlow Collection at Cisco

- DMZ Netflow Collection (4 servers)
- Data Center Netflow Collection (20+ servers)
- Query/Reporting tools (OSU Flowtools, DFlow, Netflow Report Generator)



OSU Flowtools - Netflow Collector Setup

- Tool: OSU FlowTools
 - Free
 - Developed by Ohio State University
- Examples of capabilities
 - Did 192.168.15.40 talk to 216.213.22.14?
 - What hosts and ports did 192.168.15.40 talk to?
 - Who's connecting to port TCP/6667?
 - Did anyone transfer data > 500MB to an external host?

OSU Flowtools Example - Who's Talking?

- Scenario - New botnet, variant undetected

Goal: identify all systems that 'talked' to the botnet C&C

Be glad: you have netflow collection at all your PoPs

flow.acl file
uses familiar ACL
syntax. create a list
named 'bot'

concatenate all
files from Feb 12,
2007 then filter for src
or dest of 'bot' acl

```
[mynfchost]$ head flow.acl
ip access-list standard bot permit host 69.50.180.3
ip access-list standard bot permit host 66.182.150.100

[mynfchost]$ flow-cat /var/local/flows/data/2007-02-12/ft* | flow-filter -Sbot -o -Dbot |
flow-print -f5
```

| Start DstP | End | Sif | SrcIPAddress | SrcP | Dif | DstIPa | |
|-------------------|-------------------|-----|--------------|-------|-----|--------------|----|
| 0213.08:39:49.911 | 0213.08:40:34.519 | 58 | 10.10.71.100 | 8343 | 98 | 69.50.180.3 | 7 |
| 0213.08:40:33.590 | 0213.08:40:42.294 | 98 | 69.50.180.3 | 31337 | 58 | 10.10.71.100 | 83 |

host in the
botnet!

NetFlow Report Generator – Query by IP

Netflow Report Generator

click on any of the links above the forms for help, or visit the [FAQ](#).

[Source IP:](#)

64.102.53.34

[Source Port:](#)

[Destination IP:](#)

[Destination Port:](#)

☐ Use File for Source

Upload File

☐ Use File for Destination

Upload File

[Time:](#)

1 day

[Report:](#)

html

[Netbios Resolve:](#)

[Uniq:](#)

none

[DNS Resolve:](#)

both

[Netflow Collector:](#)

all
charybdis (San Jose)
rtp-nfc
ams-nfc
syd-nfc

[Email address](#)

mnystrom@cisco.com

Run Report

64.102.53.34[xianshield.cisco.com]:48472

64.102.53.34[xianshield.cisco.com]:48472

| DESTINATION:PORT | (HOSTNAME:DOMAIN:USER) | PACKETS | TIMESTAMP |
|-----------------------------|------------------------|---------|----------------|
| 60.190.23.153[unknown]:7000 | | 1 | 1205.21:35:59. |
| 61.158.119.94[unknown]:7000 | | 1 | 1206.00:18:04. |
| 61.152.107.59[unknown]:7000 | | 1 | 1206.00:23:00. |
| 60.190.23.153[unknown]:7000 | | 1 | 1206.03:20:57. |
| 61.152.107.59[unknown]:7000 | | 1 | 1206.11:15:58. |
| 60.190.23.153[unknown]:7000 | | 1 | 1206.12:42:48. |
| 60.190.23.153[unknown]:7000 | | 1 | 1206.12:58:27. |

IP Address Data

- Critical to understanding a given incident involving 10.2.3.5
Is 10.2.3.5 in your DMZ? lab? remote access? desktop? data center?
- Make the data queryable
Commercial & open source products available
- Build the data into your security devices
SIMS - netForensics asset groups
SIMS - CS-MARS network groups
IDS - Cisco network locale variables

```
variables DC_NETWORKS address 10.2.121.0-10.2.121.255,10.3.120.0-10.3.127.255,10.4.8.0-10.4.15.255
variables DMZ_PROD_NETWORKS address 198.133.219.0-198.133.219.255
variables DMZ_LAB_NETWORKS 172.16.10.0-172.16.11.255
```

```
eventId=1168468372254753459 eventType=evIdsAlert hostId=xxx-dc-nms-4appName=sensor
appInstanceId=6718 tmTime=1178426525155 severity=1 vLan=700 Interface=ge2_1 Protocol=TCP
riskRatingValue=26 sigId=11245 sigDetails=NICK...USER" src=10.2.121.10 srcDir=DC_NETWORKS
srcport=40266 dst=208.71.169.36 dstDir=OUT
dstport=6665
```

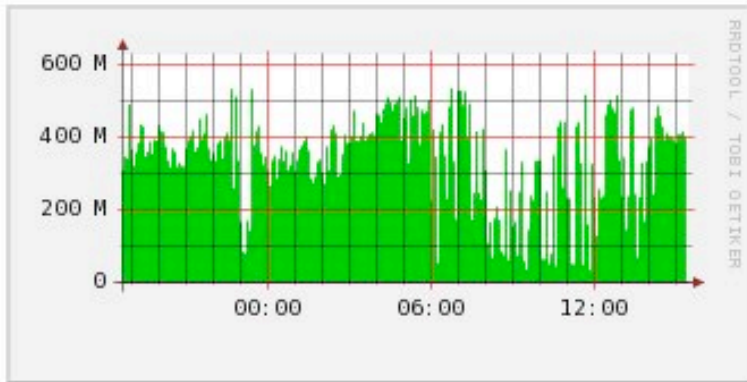
Data center host!

Network Telemetry - MRTG/RRDTool

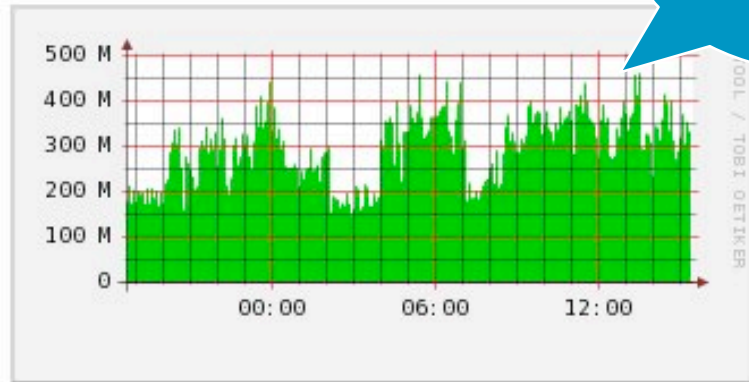
- Not just netflow, can also use SNMP to grab telemetry
- Shows data volumes between endpoints

You must understand your network traffic volume!

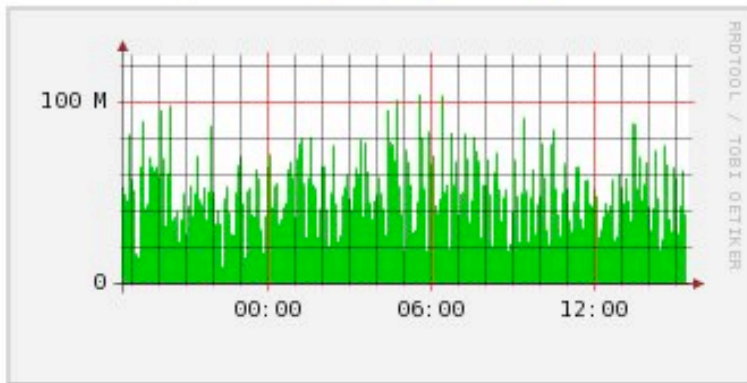
Traffic Analysis for dc-gw3 int g4/6



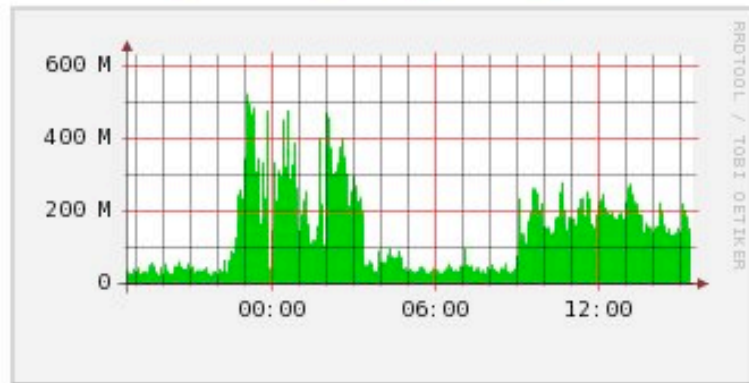
Traffic Analysis for dc-gw3 int g4/8



Traffic Analysis for dc-gw4 int g4/6



Traffic Analysis for dc-gw4 int g4/8





Step 3. Select Your Targets

1. Determine Which Assets to Monitor

- Face it: you can't monitor everything equally
- How to prioritize?

Revenue impact?

Regulatory compliance/legal obligation?

Expense reduction?

At risk?

Systems that can't be patched

Most attractive targets to hackers?

Sensitive data?

Visibility to upper management?

Manageable event rates?

- Hopefully, someone else figured this out for you

Disaster planning teams

- Which incidents can be mitigated?



Recommendation: Best Targets

1. Accesses sensitive data

- Legal compliance
- Intellectual property
- Customer sensitive data

2. Risky

Fewer controls (ACL's, poor configs, etc.)

Hard to patch (limited patch windows, high uptime requirements, custom vendor code, etc.)



3. Generates revenue

4. Produces actionable events

- Why monitor if you can't mitigate?

2. Determine Components to Monitor

- What assets are associated with the target?

host names

databases

applications

network devices

- Example: Monitor ERP system

List assets associated with system

10 clustered Linux servers

5 clustered database servers

4 “logical” application names

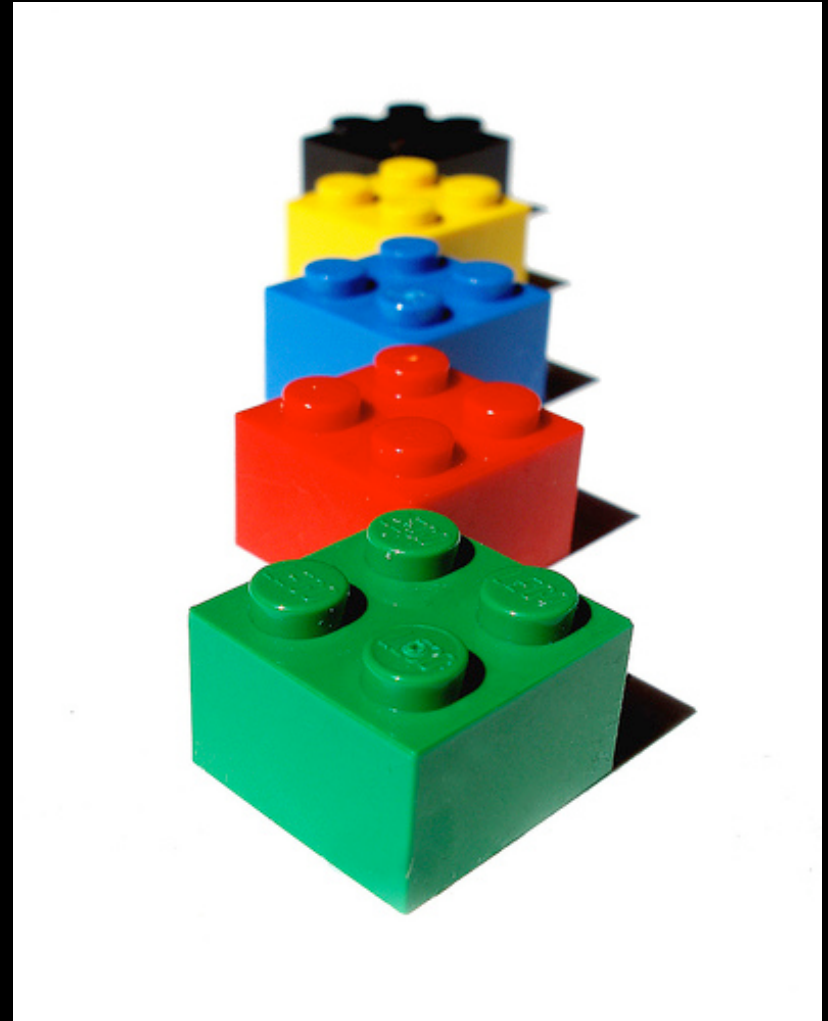
1 LDAP server

Policy: Database should only be accessed from app server

Monitor for:

Outbound connections from db

Access to DB on non SQL ports (SSH, terminal services, etc.)





Step 4. Choose Event Sources

Choosing Event Sources: What to Consider



- How will you use it?
 - For monitoring
 - For incident response
 - For investigations
- How will you collect it?
 - Pushed from device (syslog, netflow, etc.)
 - Pulled from device (SDEE, SNMP, Windows logs, etc.)
 - Detected with special equipment (IDS, etc.)
- Performance: what will it do to the sending device?
 - Can you get sufficient detail?
 - Will the support staff give it to you?

Choosing Event Sources: What to Consider (cont.)

- How much storage do you have?
- What tools will you use to read it?

SIM, log analyzer, etc.

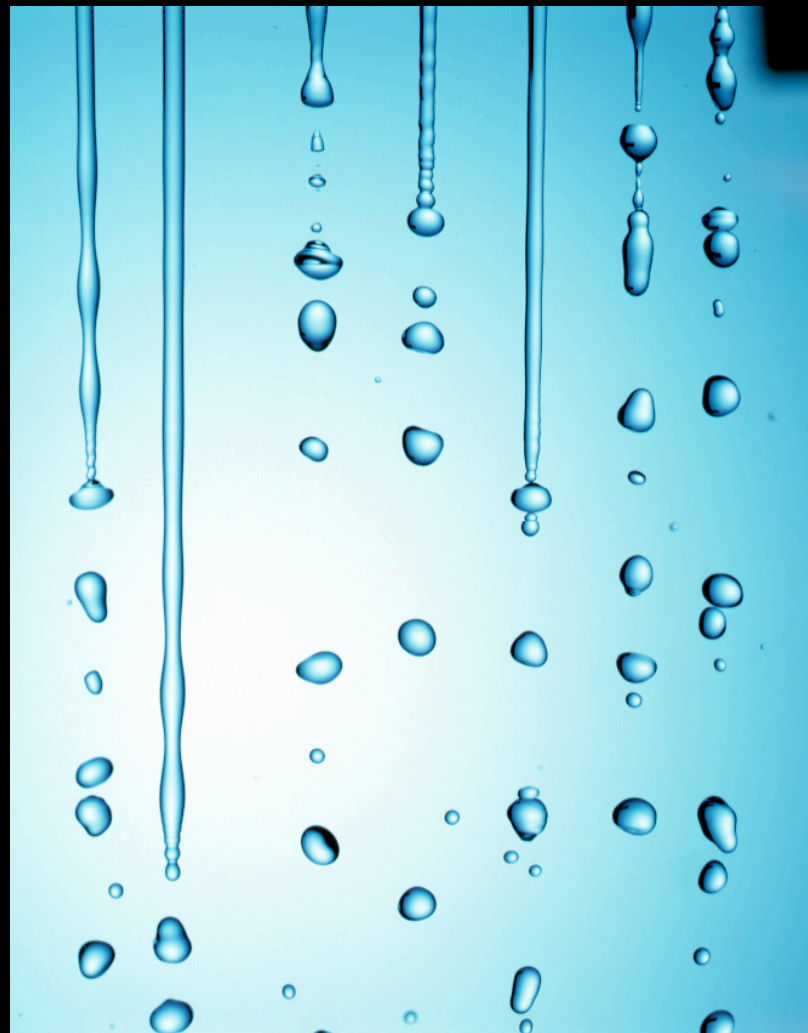
- Application specific

Can you recognize “false positive” patterns and tune them out?

Will you get enough information to act on it without a full packet-capture?

Can you identify specific incidents and how you’d see it with your event source?

Do you know what you’d do with it if there’s really an incident?



Three Best Event Sources

■ Netflow

Collect at chokepoints (data center gateways)

Cheap to collect: SJC stores 3 ISP gateways, 200k pps, 600GB storage, can query back 3 months

Free tools to collect, relay, query

OSU FlowTools, nfdump/nfsen, etc.

■ Network IDS

Collect at chokepoints (data center gateways)

No agents or feeds taxing end systems

■ Host logs

Unix: syslog

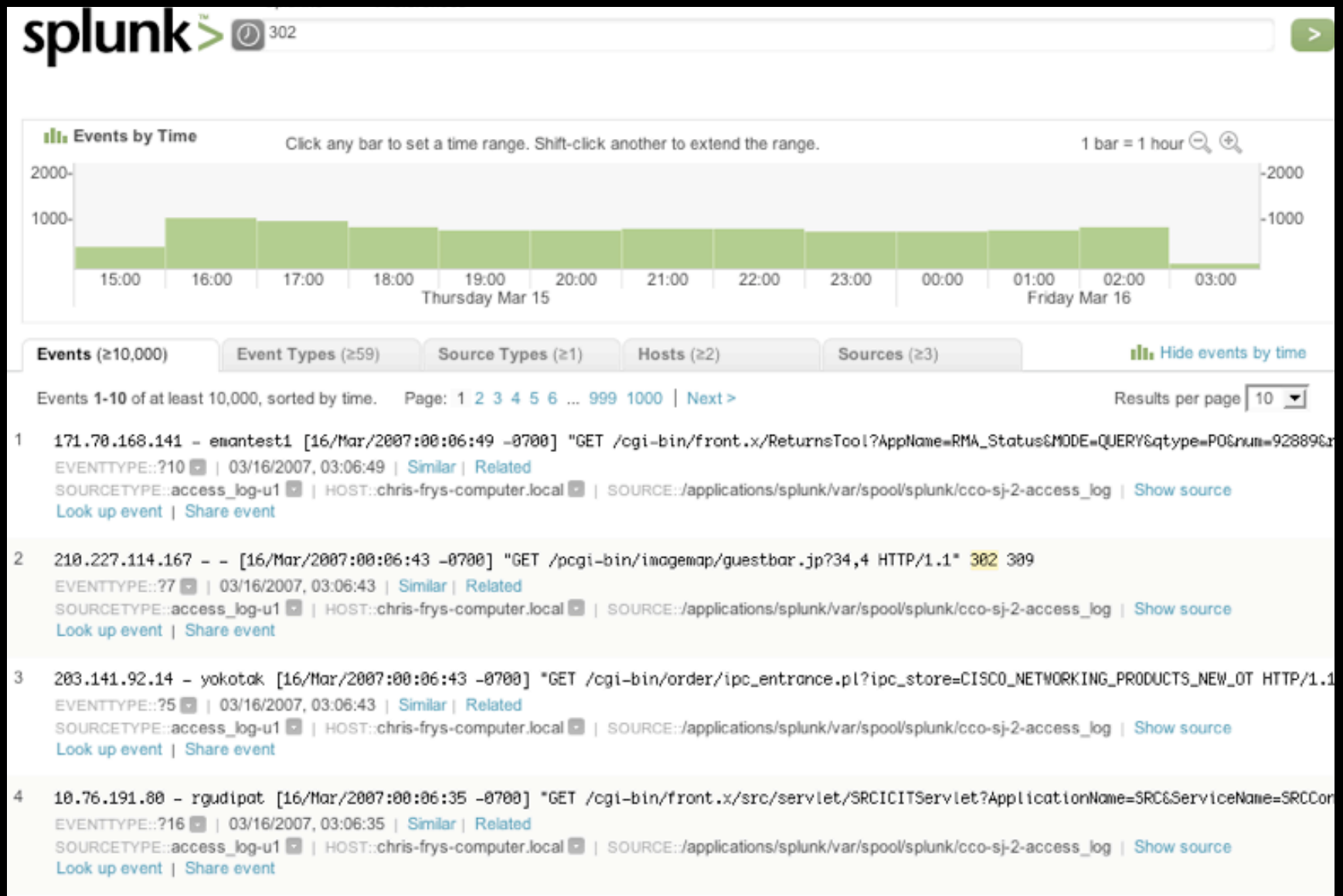
Collect common services via syslog (web servers, mail servers, etc.)

Collect with syslog relay/collector

syslog-ng, splunk, etc.

Collect Windows logs into same infra with Snare agents

Searching Through Logs w/Splunk



Searching Through Logs w/Sawmill

Sawmill Lite [Trial, 30 days left] Profile: test Logged in as 'cfry' Admin | Logout | Help | About

Calendar Date Range Printer Friendly Update Database | Rebuild Database

▼ Date and time
▼ Content
Pages/directories
Pages
File types
▼ Visitor demographics
Hostnames
Domain descriptions
Geographic locations
Authenticated users
▼ Visitor systems
▼ Other
Server responses
▼ Sessions
• Sessions overview
Entry pages
Exit pages
Paths through a page
Session paths
Session pages
Session users
Individual sessions
Single-page Summary

Individual sessions Row Numbers Zoom Options Export | Table Options

Row 1 - 10 of 24,556 11-20 > >>> Start row: 1 Number of rows: ▼

| Session ID | User | ▼ Events | 0 - 100 % | Start Time | End Time |
|---------------------------------------|-----------------|-----------|-----------|----------------------|----------------------|
| 1 192.63.136.118-2007-03-15:12:25:57 | 192.63.136.118 | 122 0.2 % | | 15/Mar/2007 12:25:57 | 15/Mar/2007 14:00:12 |
| 2 192.63.136.118-2007-03-15:09:28:50 | 192.63.136.118 | 100 0.1 % | | 15/Mar/2007 09:28:50 | 15/Mar/2007 10:29:51 |
| 3 71.168.213.78-2007-03-15:16:02:31 | 71.168.213.78 | 98 0.1 % | | 15/Mar/2007 16:02:31 | 15/Mar/2007 17:28:21 |
| 4 203.197.142.1-2007-03-15:22:06:34 | 203.197.142.1 | 92 0.1 % | | 15/Mar/2007 22:06:34 | 16/Mar/2007 00:05:38 |
| 5 209.47.179.250-2007-03-15:05:05:06 | 209.47.179.250 | 88 0.1 % | | 15/Mar/2007 05:05:06 | 15/Mar/2007 06:40:45 |
| 6 152.102.1.107-2007-03-15:00:13:01 | 152.102.1.107 | 80 0.1 % | | 15/Mar/2007 00:13:01 | 15/Mar/2007 01:04:54 |
| 7 166.42.249.221-2007-03-15:10:13:12 | 166.42.249.221 | 79 0.1 % | | 15/Mar/2007 10:13:12 | 15/Mar/2007 11:55:25 |
| 8 38.99.222.242-2007-03-15:09:55:43 | 38.99.222.242 | 75 0.1 % | | 15/Mar/2007 09:55:43 | 15/Mar/2007 11:06:18 |
| 9 208.214.139.134-2007-03-15:12:46:24 | 208.214.139.134 | 75 0.1 % | | 15/Mar/2007 12:46:24 | 15/Mar/2007 14:15:08 |

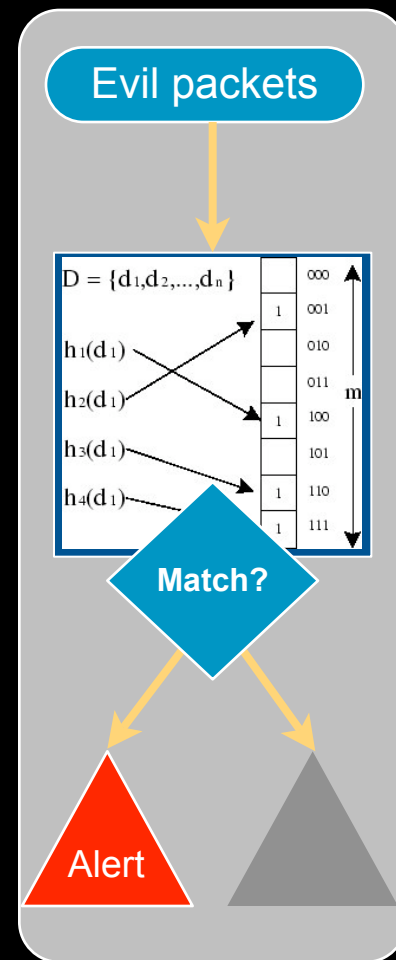
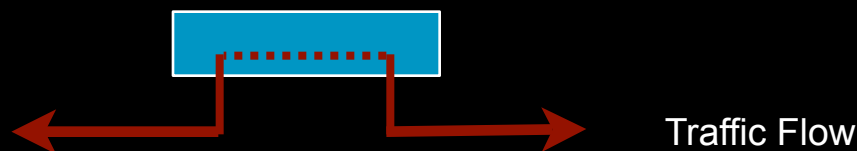


IDS/IPS Refresher

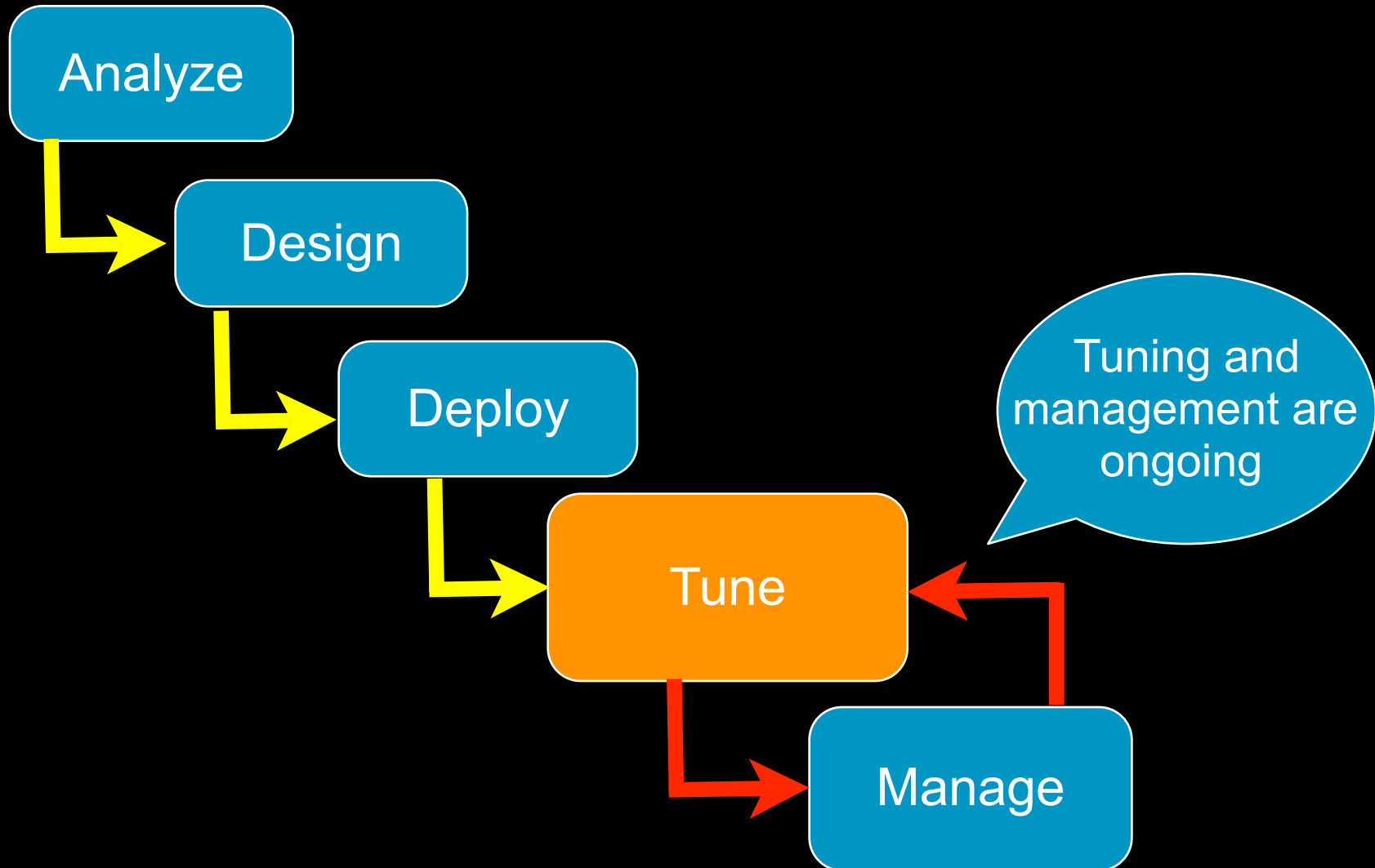
- IDS - Intrusion Detection System
passive network traffic monitoring
limited actions, mostly for alerting



- IPS - Intrusion Prevention System
inline network traffic monitoring
alerting + ability to drop packets



IDS - basic deployment steps

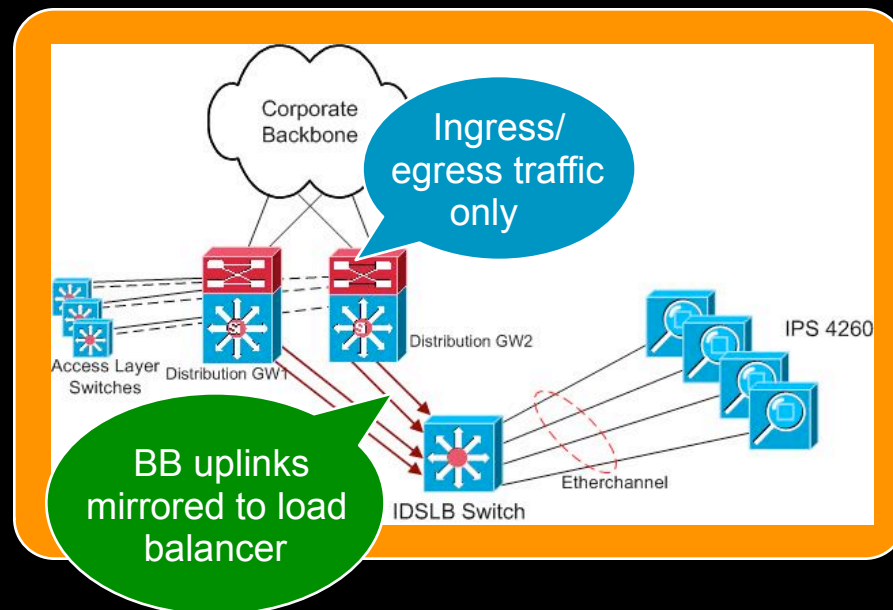
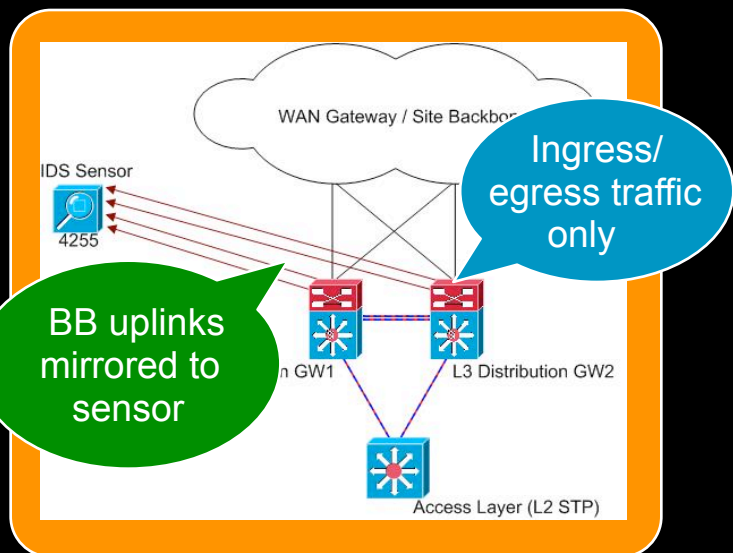


Setup IDS

- Avoid asymmetry in your *traffic view*!
- Minimize the number of platforms and designs

Two different designs: small vs. large data centers

Distribution layer router uplink traffic ideal



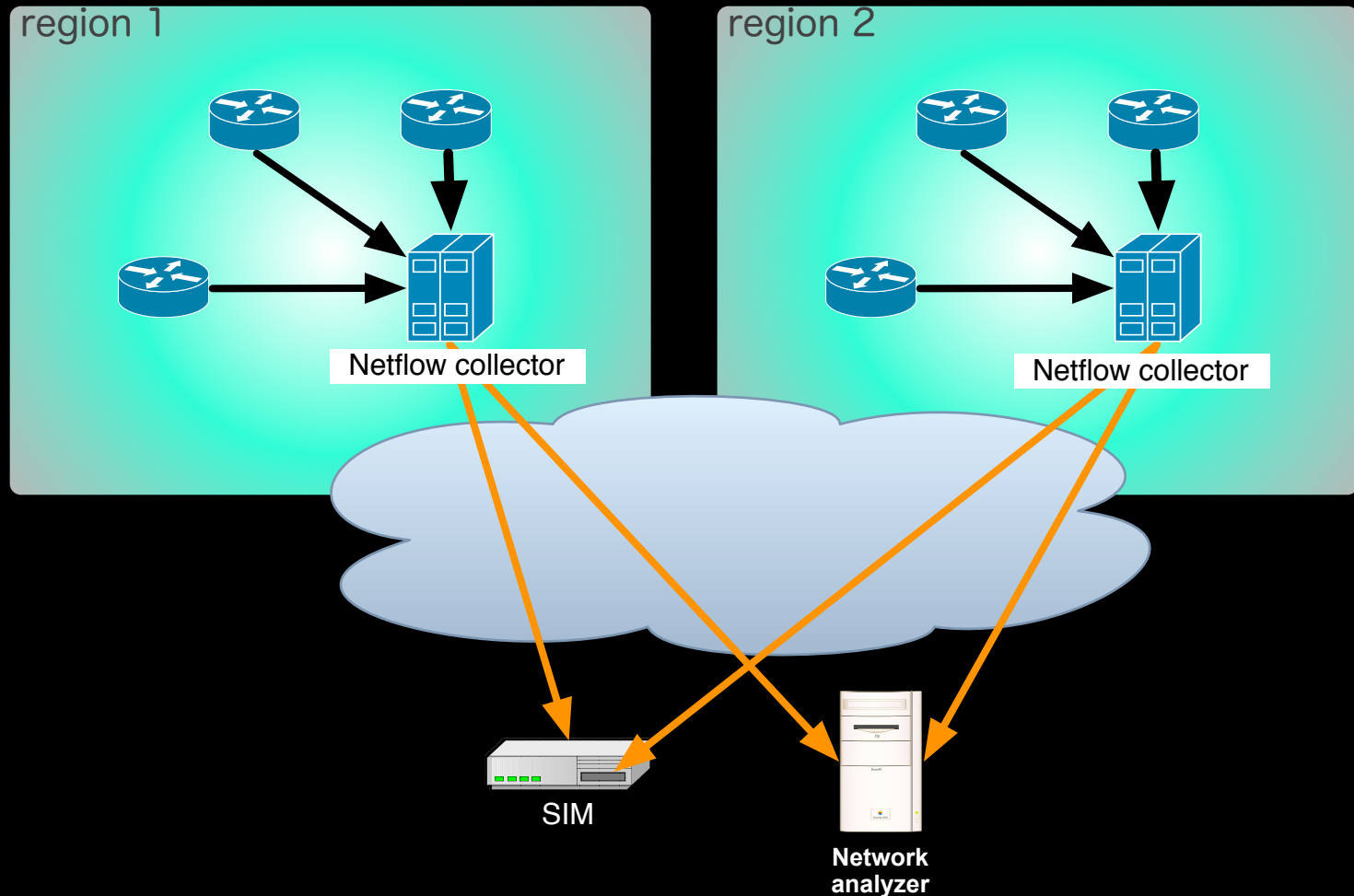
Feed Netflow to SIMs and Other Tools

- Feed Netflow to every tool that will use it

MARS,
PeakFlow,
etc.

- Regionalize deployment

minimize
sending
over
network



Host Syslog

- Capture, store, and relay with syslog-ng

- For monitoring, be sure your SIM can parse events

- Deploy standard template (syslog.conf)

- Key events to log

authentication logs

authorization logs (sudo, su, etc.)

daemon status logs (know when they stop/start)

security application logs (tcpwrappers, portsentry, etc.)

- Windows logging

Agents can relay events via syslog

Very noisy, grab only important events

```
wally ~ # ./chroma.rb tail -f /var/log/messages
Dec  2 16:55:01 wally cron[25120]: (root) CMD (mr
Dec  2 17:00:01 wally cron[25285]: (root) CMD (te
Dec  2 17:00:01 wally cron[25287]: (root) CMD (rm
Dec  2 17:00:01 wally cron[25289]: (agorf) CMD (g
Dec  2 17:00:01 wally cron[25291]: (agorf) CMD (g
Dec  2 17:00:01 wally cron[25293]: (agorf) CMD (g
Dec  2 17:00:01 wally cron[25295]: (root) CMD (mr
Dec  2 17:00:02 wally cron[25307]: (root) CMD (mr
Dec  2 17:05:01 wally cron[25451]: (root) CMD (mr
Dec  2 17:05:01 wally cron[25453]: (root) CMD (mr
Dec  2 17:10:01 wally cron[25612]: (root) CMD (te
Dec  2 17:10:01 wally cron[25614]: (agorf) CMD (g
Dec  2 17:10:01 wally cron[25616]: (root) CMD (mr
Dec  2 17:10:01 wally cron[25618]: (root) CMD (mr
Dec  2 17:10:54 wally uptimed: moving up to posit
Dec  2 17:15:01 wally cron[25657]: (root) CMD (mr
Dec  2 17:15:01 wally cron[25659]: (root) CMD (mr
```

| EventID | Title |
|-----------|---------------------|
| 528 | User Logon |
| 529 - 537 | Logon Failure |
| 538 | User Logoff |
| 612 | Audit Policy Change |
| 517 | Audit Log Cleared |

Other Logs



- Web server logs

Can verify and elaborate attacks

Use HTTP status codes to determine if IDS alert really worked

Can provide URL details during attack

Apache

Send as syslog via httpd.conf setting

IIS

Send as syslog via MonitorWare Agent

- App server logs

Find way to relay as syslog

Send via SNMP events

Pull via SQL queries

- Oracle logs

Pull logs from AUD\$ table via SQL

Internal vs. Perimeter (DMZ) Monitoring



What's the difference?

Number of Services/Protocols



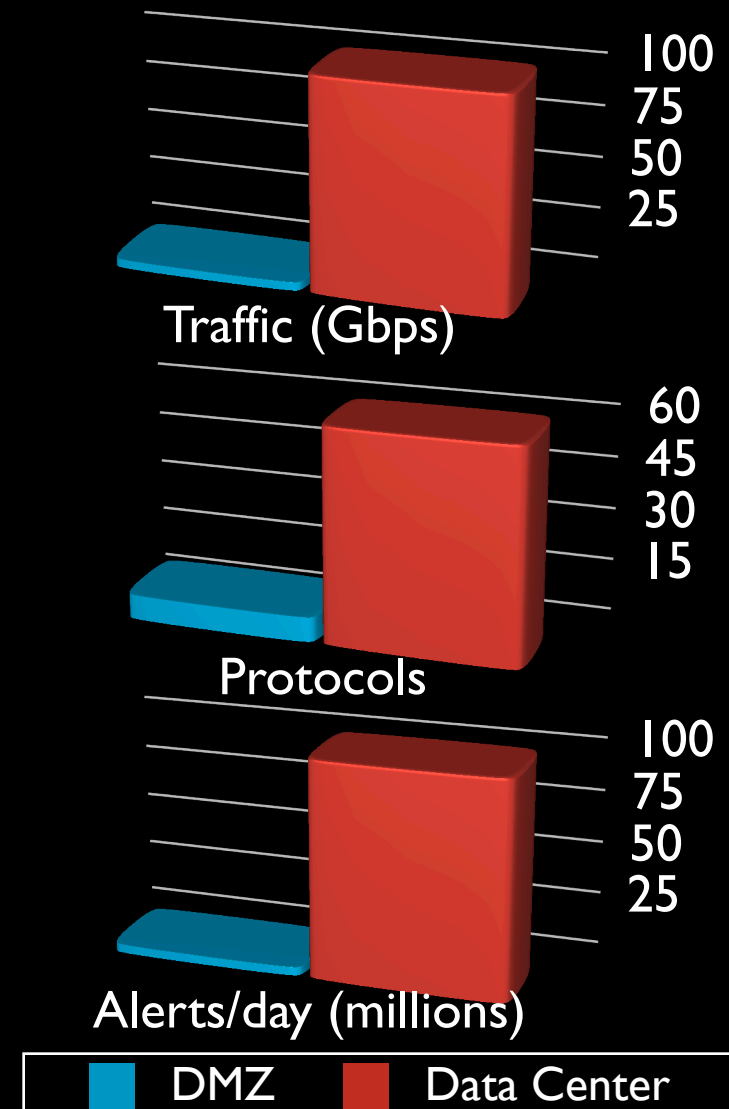
- Many more false positives sources
- Tuning more complex

A good relationship with IT application and service owners is key

Enterprise Datacenter Monitoring

Complications / Difficulties

- **Traffic:** 100+ Gbps globally vs. 4 Gbps outside
- **Protocols:** Higher number of services/protocols increases variety and complexity of tuning
- **Alerts:** Untuned sensor in large datacenter generates > 100 million alerts/day



Enterprise Datacenter Monitoring

Complications / Difficulties (continued)

- **Higher availability expectations**

Enterprise data centers have very high availability requirements

Inline “IPS” a hard sell, most hardware not properly redundant

We don’t use inline IPS

- **False positives**

Difficult and time consuming to identify

Key: good relationship with IT application and service owners

- **Relatively new technology**

Not well understood by IDS & SIMs yet

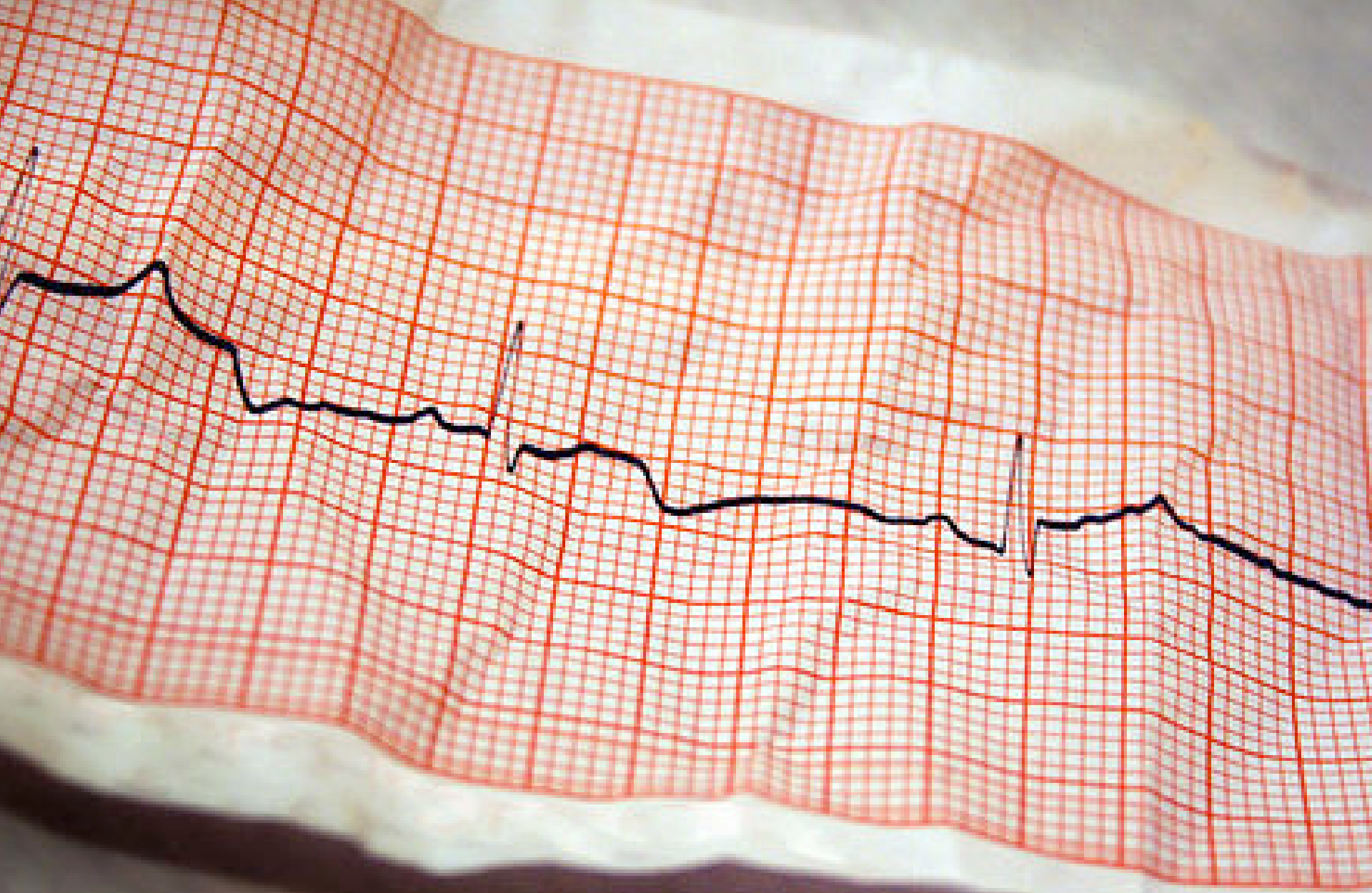
Limited signature base

Most signatures based on Internet attacks

False Positives - Examples

- SigID 3320 - ADMIN\$ access
- SigID 3337 - Windows RPC Race Condition
- SigID 5722 Google Appliance ProxyStyleSheet Cmd Exec
- SigID 3653 Multiple Rapid SSH Connections

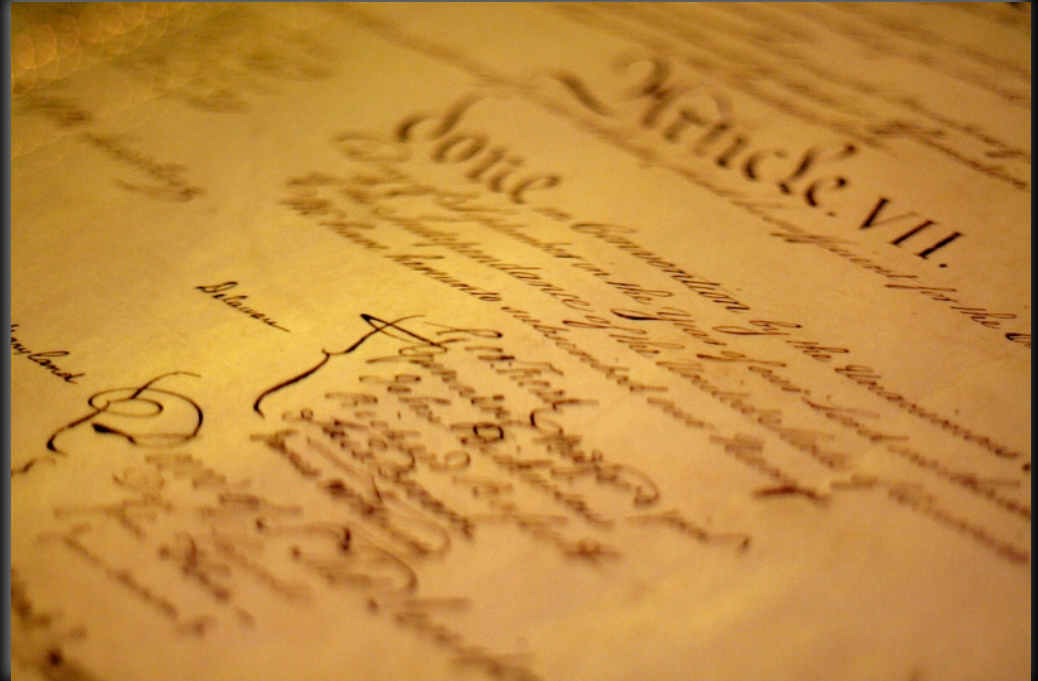
Each of these required that we contact the IT application or system owners to verify false positive.



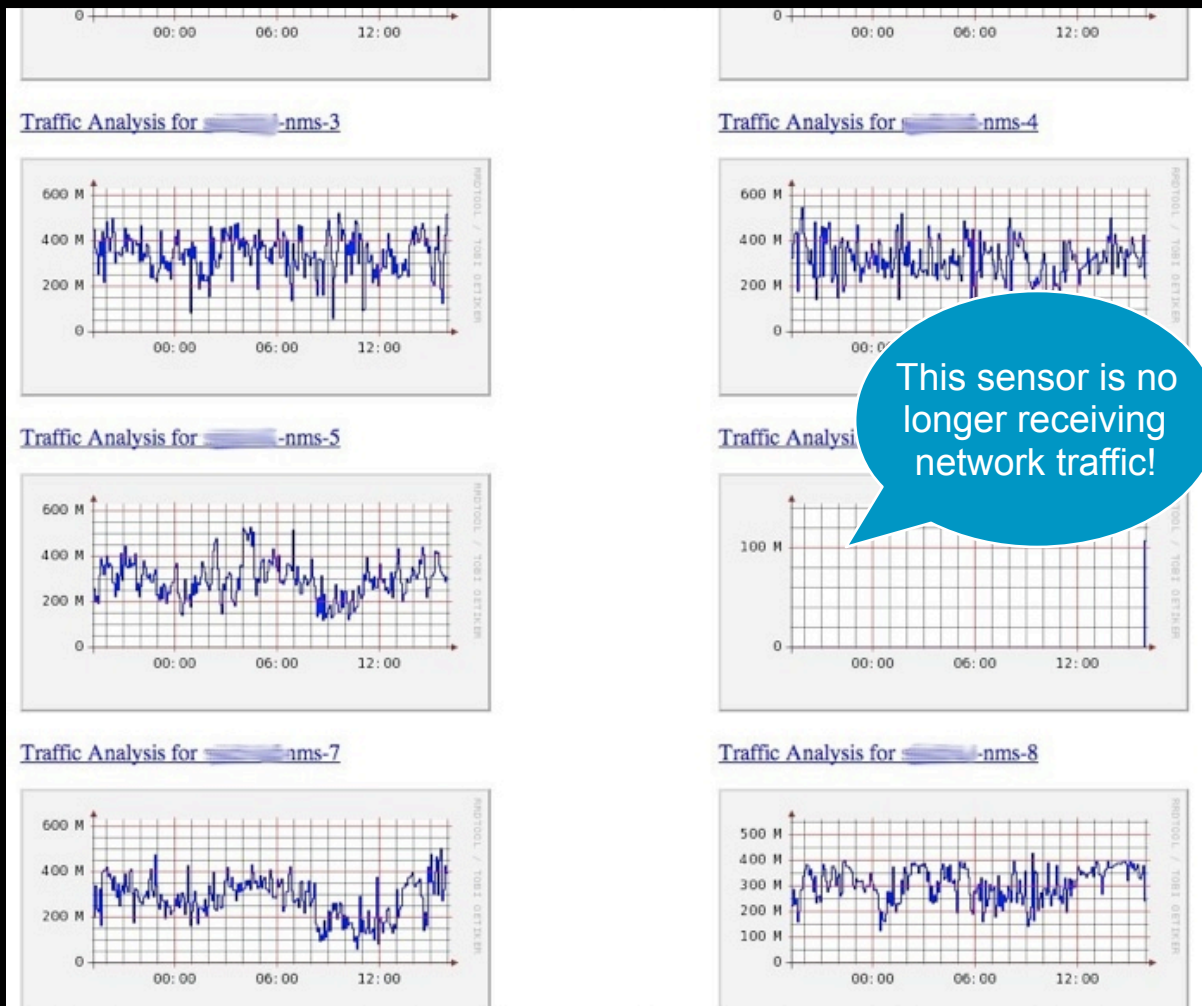
Step 6. Maintain & Troubleshoot

Maintain Documented Commitments

- Document agreements with IT
 - Fixed timelines
 - Expectations (SLAs, OS patching, etc)
 - Refresh commitments every year
- Review assets regularly
 - Look for new assets, new feeds, replaced hosts, etc.
 - Check for feeds/hosts that may have changed/ disappeared
 - Check for ownership changes due to re-orgs



Maintain IDS Feeds



- Monitor your IDS sensor uplinks sensor processes
- Watch for spikes/drops in sensor alert volume
- Have monitoring staff monitor feeds

Verify Feeds

- Syslog feed verification

Script awk to grab hostnames of systems that syslog daily and do a diff

Ask IT to use a daily cron to re-set syslog.conf on servers

- Netflow feed verification

tcpdump -i eth0 port 2060 -c 1000 | grep gw | awk '{print \$2}' | sort | uniq

```
May 16 07:57:40 flanders-mac com.apple.SecurityServer: Succeeded authorizing right system.preferences/System Preferences.app for authorization created by /Applications/System Preferences.app
May 16 07:57:41 flanders-mac com.apple.SecurityServer: Succeeded authorizing right system.preferences/Library/PrivateFrameworks/Admin.framework/Resources/writeconfig for authorization created by /preferences.app.
May 16 07:57:41 flanders-mac com.apple.SecurityServer: Succeeded authorizing right system.preferences/Library/PrivateFrameworks/Admin.framework/Resources/writeconfig for authorization created by /preferences.app.
May 16 09:51:40 flanders-mac com.apple.SecurityServer: Succeeded authorizing right system.preferences/System Preferences.app for authorization created by /Applications/System Preferences.app
May 16 09:51:41 flanders-mac com.apple.SecurityServer: Succeeded authorizing right system.preferences/Library/PrivateFrameworks/Admin.framework/Resources/writeconfig for authorization created by /preferences.app.
May 16 09:51:41 flanders-mac com.apple.SecurityServer: Succeeded authorizing right system.preferences/Library/PrivateFrameworks/Admin.framework/Resources/writeconfig for authorization created by /preferences.app.
May 16 15:50:07 flanders-mac com.apple.SecurityServer: authinternal authenticated user martinny
May 16 15:50:07 flanders-mac com.apple.SecurityServer: uid 501 succeeded authenticating as user for right system.login.screensaver.
May 16 15:50:07 flanders-mac com.apple.SecurityServer: Succeeded authorizing right system.login/System/Library/CoreServices/loginwindow.app for authorization created by /System/Library/CoreServices/loginwindow.app
May 16 17:22:36 flanders-mac sshd[17844]: Could not write ident string to UNKNOWN
May 16 17:53:16 flanders-mac com.apple.SecurityServer: authinternal authenticated user martinny
May 16 17:53:16 flanders-mac com.apple.SecurityServer: Succeeded authorizing right system.login/sudo for authorization created by /usr/bin/sudo.
```


Lessons Learned

- Start small

- Too many events at once is overwhelming

- Understand/tune each source before adding more

- Understand “normal” traffic thoroughly before moving on

- Avoid alerting on false-positives

- Use a SIM

- Event correlation, false positive reduction

- Choose carefully what you want to monitor

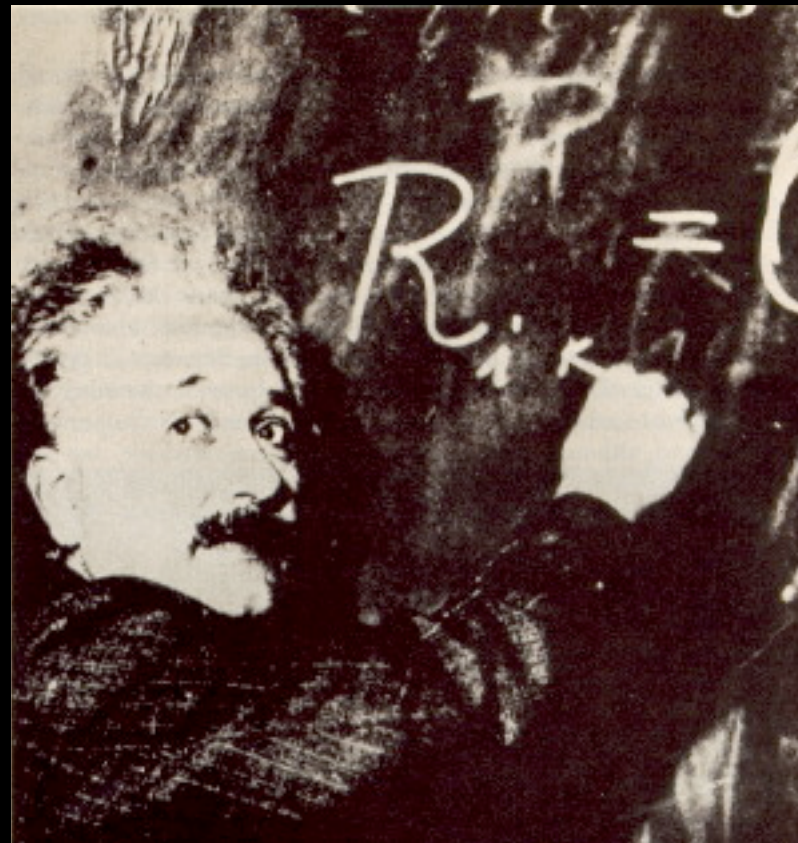
- ...or you'll waste your time chasing false positives

- Use defined playbooks, escalation procedures

- Have allies in the IT support teams

- Network support, DBA's, webmasters, etc.

- They can explain/remediate issues you find





6. Troubleshoot

5. Feed and tune

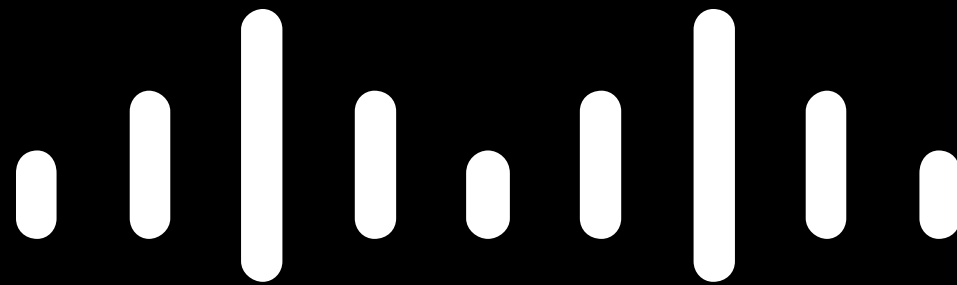
4. Choose event sources

3. Select targets

2. Know the network

1. Know your policy

6 steps to improve your security monitoring



CISCO