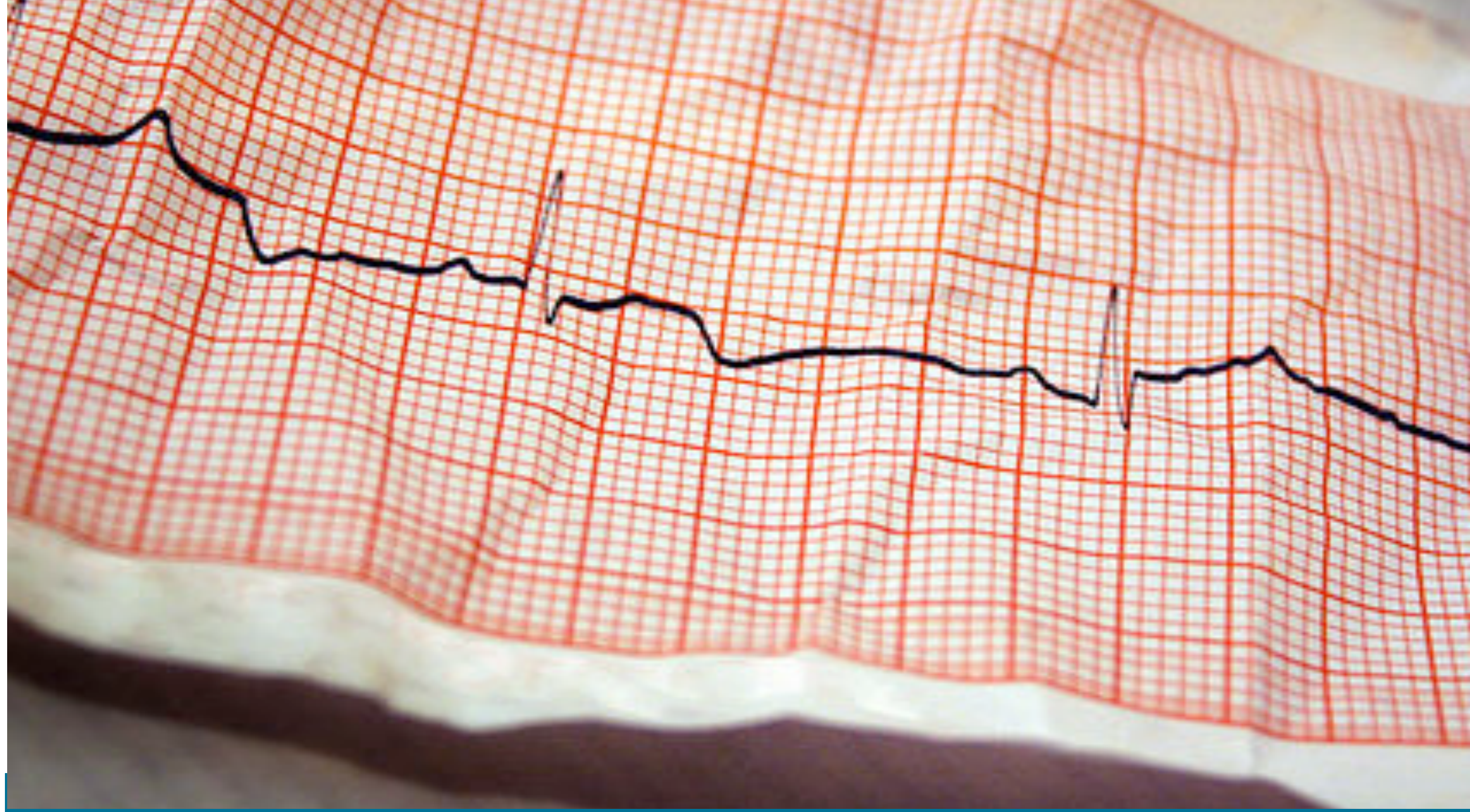


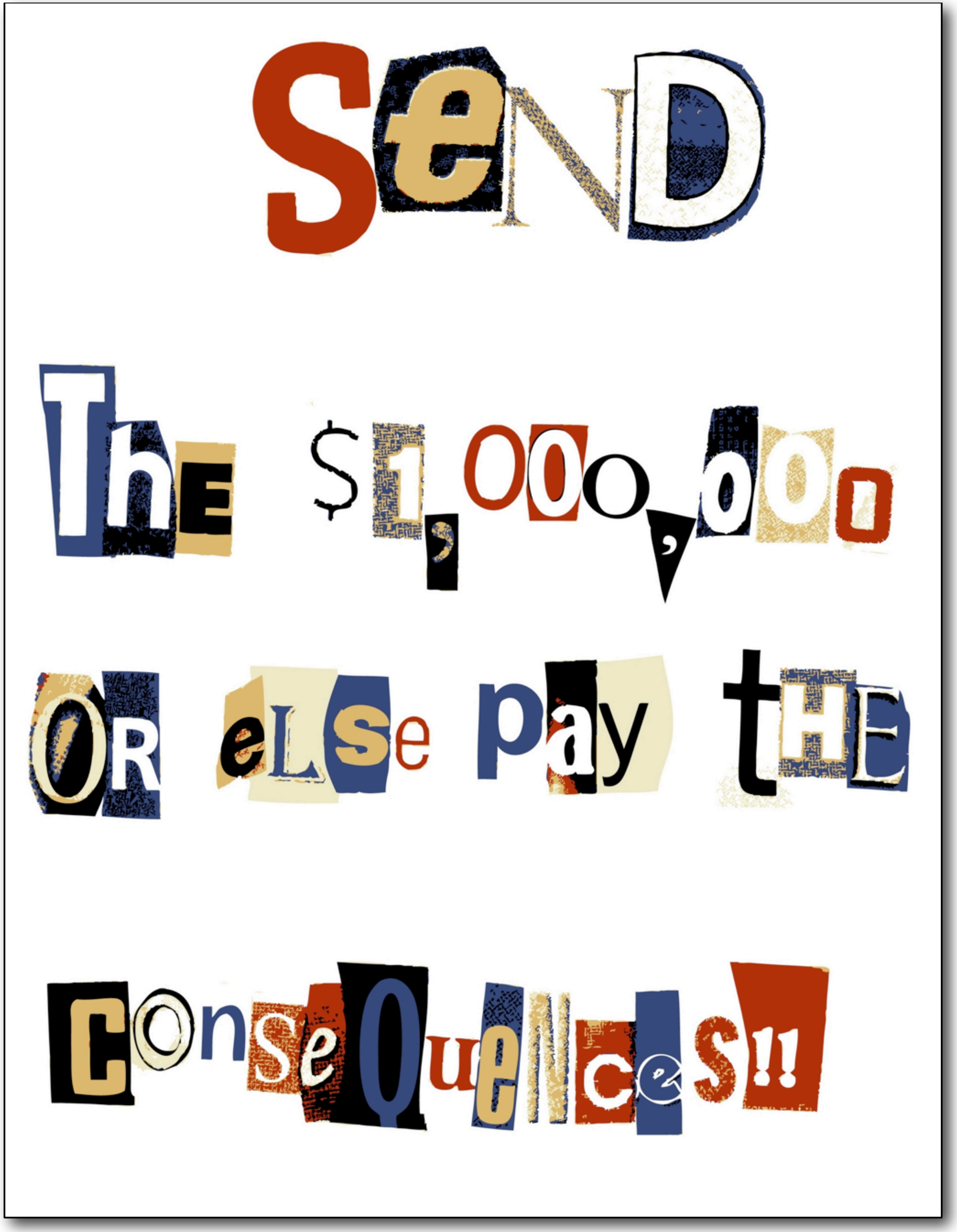
Missing Clues

How to Prevent Critical Gaps in Your Security Monitoring

Dave Schwartzburg (daschwar@cisco.com)

Martin G. Nystrom (diddly@cisco.com)

Cisco CSIRT



SEND

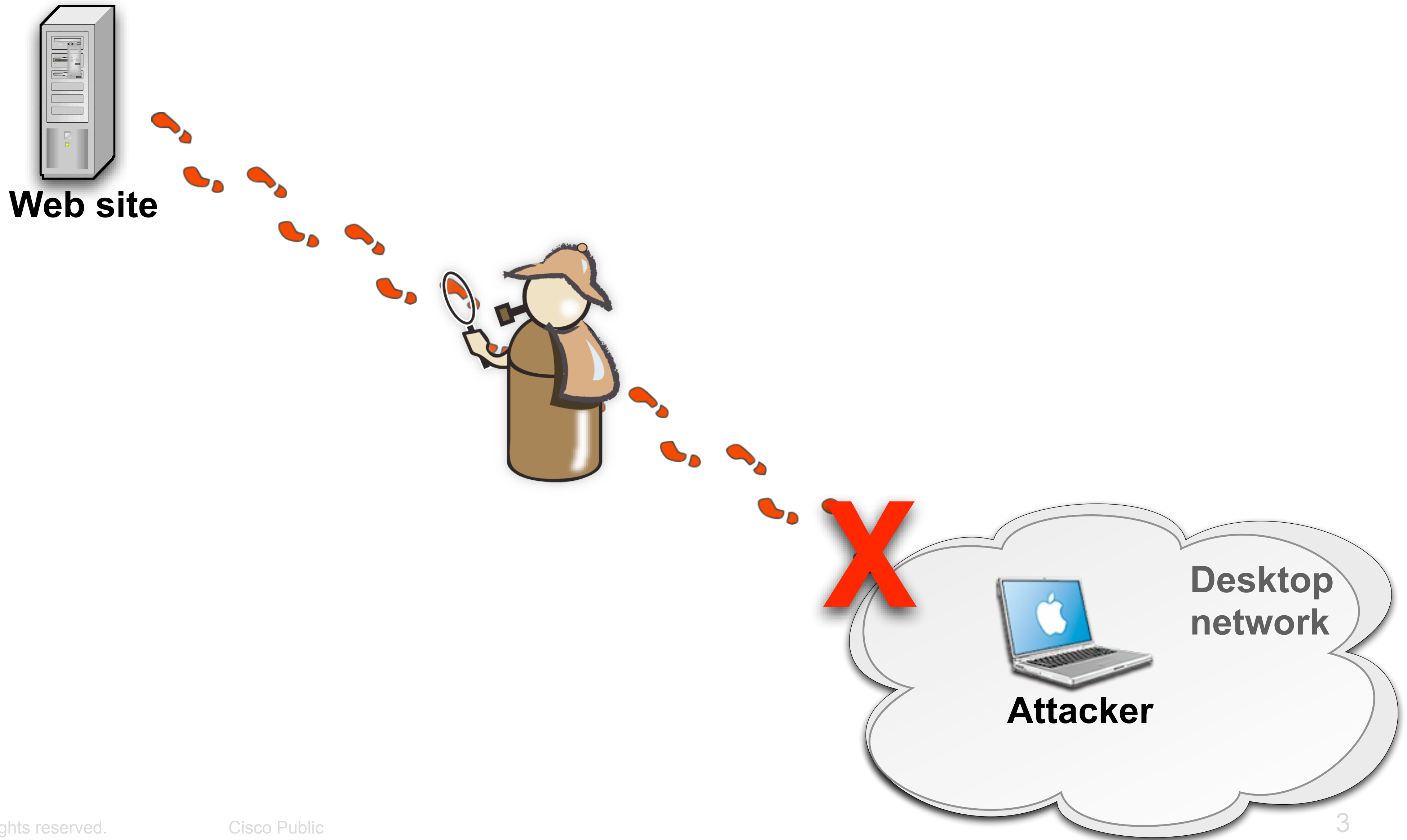
The $1,000,000

OR else pay the

consequences!!

Investigation Hit Dead End

- NetFlow records correlated to desktop subnet
- No DHCP logs to trace who had IP address at that time..
- Dead End!



Today’s Outline

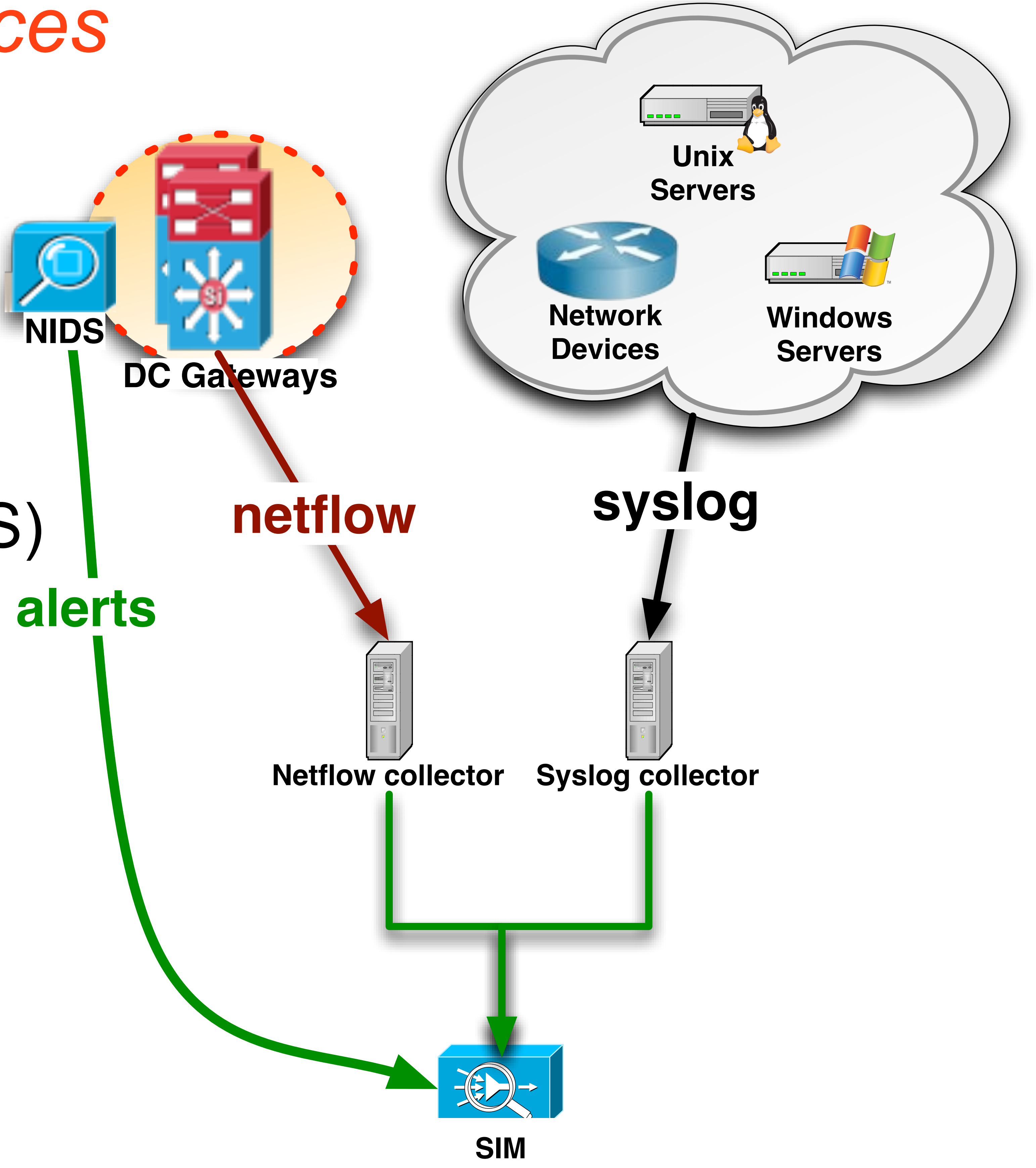
- Review security monitoring architecture
- Maintain configurations
  - Policies, agreements
  - Automation
- Monitor event sources
- System monitoring solutions
  - Using Nagios
- Closing
  - Watching for new event sources
  - Implementation checklist

Review Security Monitoring Architecture

Review Security Monitoring Architecture

Common Event Sources

- Network intrusion detection systems (NIDS)
- NetFlow
- Server logs
  - Unix (syslog)
  - Windows event logs
- Network device logs
- Application logs (web server, etc.)
- Database audit records



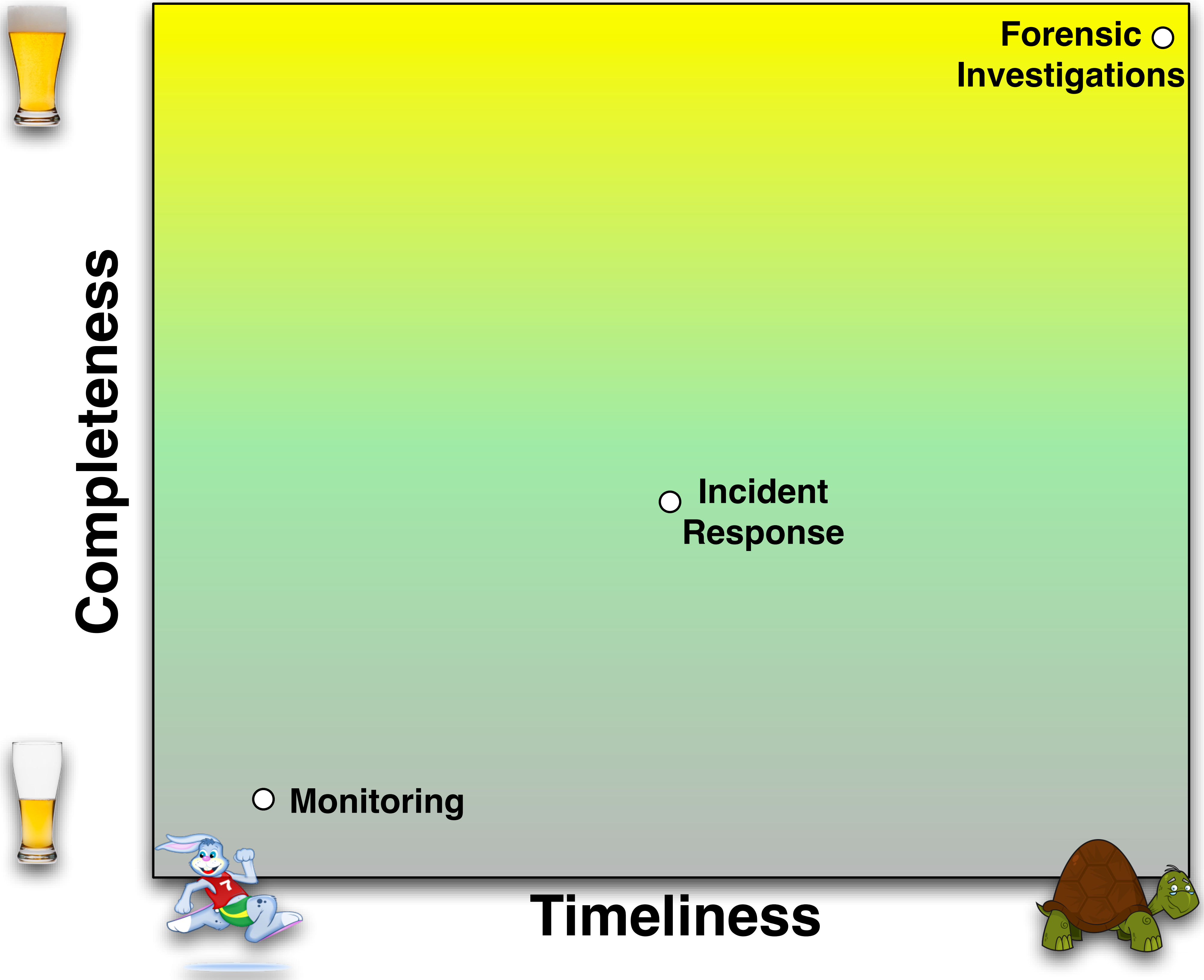
Review Security Monitoring Architecture

Common Interruptions to Event Flows

Problems	**Examples**
Device misconfiguration	• Router spans changed • NetFlow exports removed • Syslog.conf changed by sysadmin
Resource exhaustion	• Disk full • Memory full • Insufficient CPU
Network problems	• Link saturated • Firewall ACLs changed • IP address changes

Review Security Monitoring Architecture

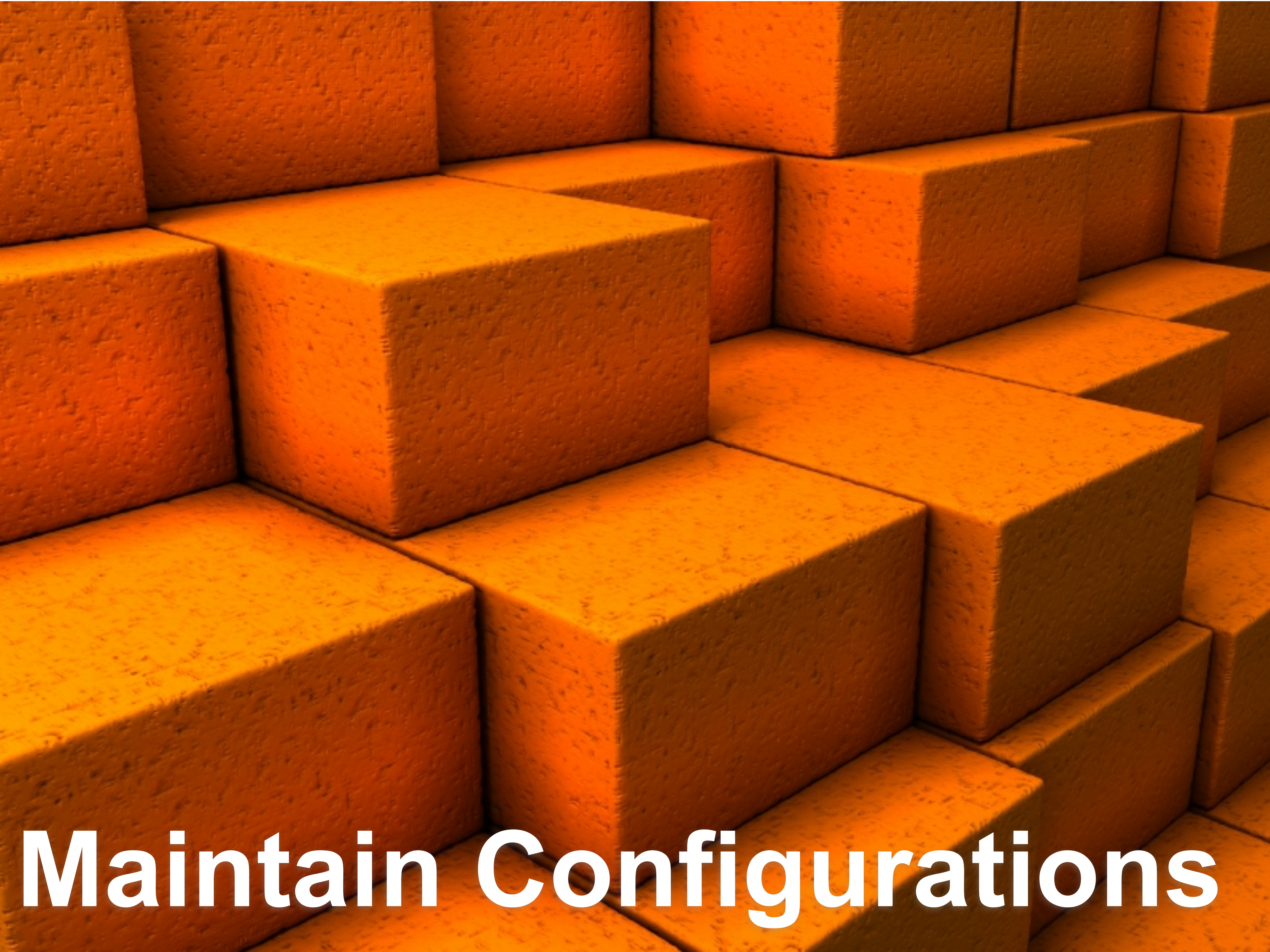
Retention of Event Data



Review System Monitoring Architecture

Events from Host and Network Devices

Device Type	Events
All	Authentication
	Config changes
	Service stops/starts
Firewalls	Permit/deny records
Remote access	IP assignments to user/machine
Cache engines	Content access
DHCP Servers	IP assignments to user/machine
Wireless access	IP assignments to user/machine



Maintain Configurations

Maintain Configurations
Document Commitments

- **SLA**: Document agreements with support teams
  - Expectations
    - Patching
    - Change notification
    - Timelines
  - Refresh every year
- Review assets regularly
  - Look for new assets, new feeds, replaced hosts, etc.
  - Check for feeds/hosts that have changed/disappeared
  - Check for ownership changes due to re-orgs

Maintain Configurations
Policies

- Event sources must log to remote servers
- Store events read-only
  - Prevent attacker from erasing logs
- Policy requires:
  - Who: which servers should log
  - What must be logged
  - Where logs must go

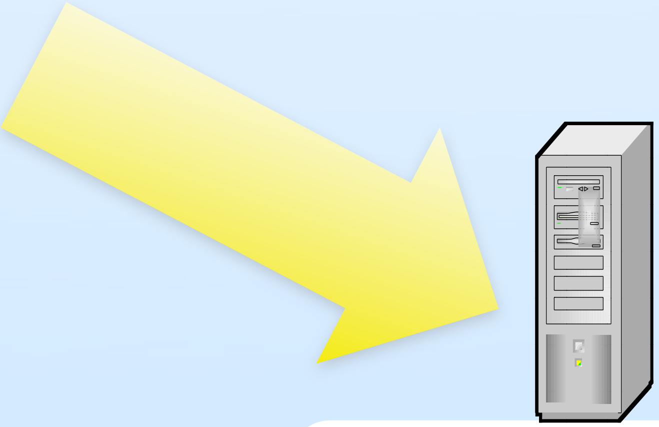
Maintain Configurations
Automated Config Management

- Ensures logging (and other things) conform to policy
- Improves consistency
- How to:
  - Build and deploy standard template
  - Leverage existing frameworks
    - Red Hat Network - package deployment
    - Microsoft System Center Configuration Manager
  - ...or build custom framework
    - Cisco autoconfig templates

Maintain Configurations

Example Syslog Template

```
# Sample section of syslog.conf to enable remote logging
local2.notice   /var/log/sudolog
local2.notice   @10.83.4.102
local3.info     /var/adm/ssh.log
local3.info     @10.83.4.102
local4.info     /var/adm/tcpwrap.log
local4.info     @10.83.4.102
local7.info     /var/adm/portsentry.log
local7.info     @10.83.4.102
*.err;kern.debug;daemon.notice;mail.crit
@10.83.4.102
auth.notice     /var/log/authlog
auth.notice     @@10.83.4.102
```



Syslog collector
10.83.4.102

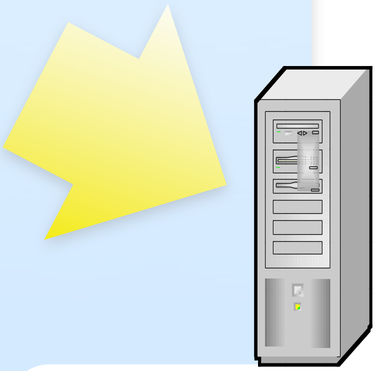
Maintain Configurations

Example Router Config Template

```
# Setup NetFlow export to our
# NetFlow collector at 10.83.4.99
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.83.4.99 2055
```

NetFlow collector
10.83.4.99

```
# Setup logging for certain events to our
# event log collector at 10.83.4.102
logging facility auth
logging facility daemon
logging trap informational
logging host 10.83.4.102
```



Syslog collector
10.83.4.102

NET FLOW
NIDS
HOST LOGS

Monitor Event Sources

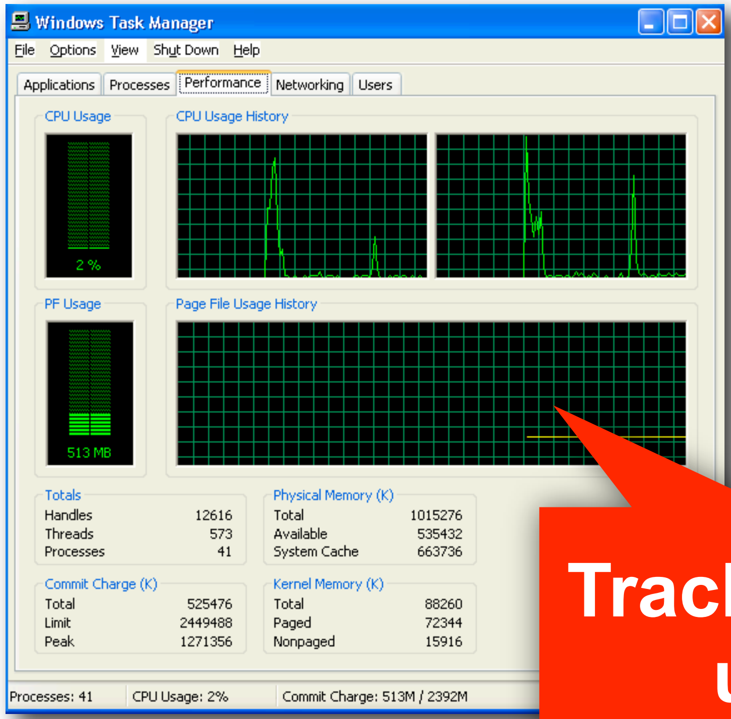
Monitor Event Sources

Health Monitoring -- Common Problems

- Disk space filling up
- Memory & swap filling up
- Maxing out CPU (load)
- System crash
- Defunct/zombie processes

Monitor Event Sources

Health Monitoring



Totals
Handles 12616
Threads 573
Processes 41

Physical Memory (K)
Total 1015276
Available 535432
System Cache 663736

Commit Charge (K)
Total 525476
Limit 2449488
Peak 1271356

Kernel Memory (K)
Total 88260
Paged 72344
Nonpaged 15916

Processes: 41 CPU Usage: 2% Commit Charge: 513M / 2392M

Track memory usage

```
test-gw1>show proc
CPU utilization for five seconds: 2%/0%; one minute: 0%; five minutes: 0%
 PID QTy       PC Runtime (ms)    Invoked   uSecs    Stacks TTY Process
   1 Cwe 6003581C             72        246        29 5484/6000   0 Chunk Manager
   2 Csp 60B76818          16392    6145                      00   0 Load Meter
   3 Mwe 627D8898              0                              00   0 chkpt message ha
   4 Mwe 623E45B0              0                             000   0 EDDRI_MAIN
   5 Lst 60032B70       51948052    3224                      00   0 Check heaps
```

Monitor CPU utilization

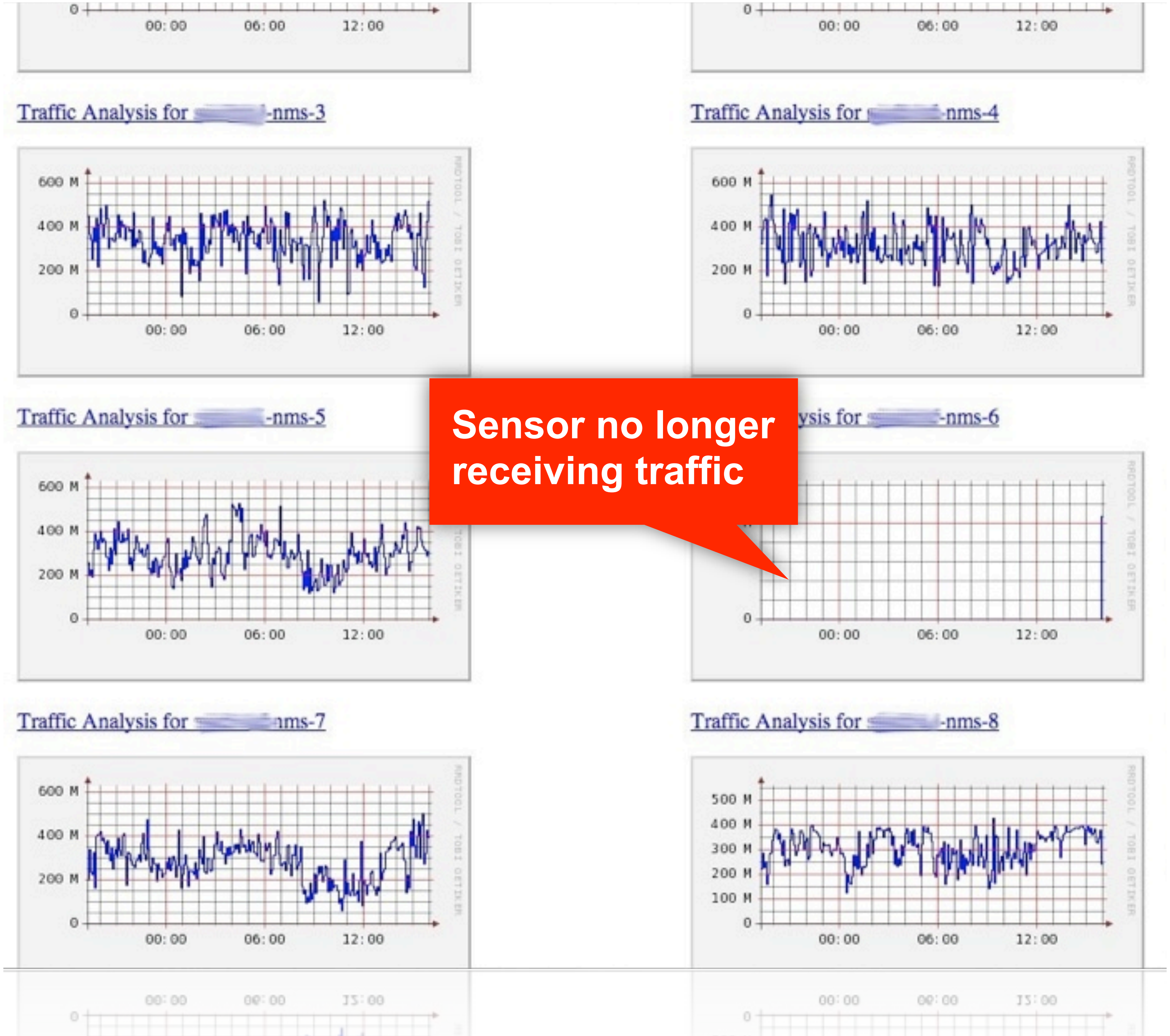
Watch for too many defunct processes

```
[netflow@blanco-nfc-1 ~]# ps auxww | grep -i z
USER        PID %CPU %MEM   VSZ  RSS TTY      STAT START   TIME COMMAND

netflow  14644  0.0  0.0     0    0 ?        Z    Sep19   0:02 [find] <defunct>
netflow  27622  0.0  0.0     0    0 ?        Z    Sep20   0:02 [find] <defunct>
```

Monitor Event Sources

NIDS - Common Problems

- Resource exhaustion
- Running but not generating events
- NIDS becomes unresponsive
- Spans or trunks change
- Too much traffic to inspect



Sensor no longer receiving traffic

Traffic Analysis for [redacted]-nms-3
Traffic Analysis for [redacted]-nms-4
Traffic Analysis for [redacted]-nms-5
Traffic Analysis for [redacted]-nms-6
Traffic Analysis for [redacted]-nms-7
Traffic Analysis for [redacted]-nms-8
600 M
400 M
200 M
0
500 M
300 M
100 M
00:00
06:00
12:00
RRDTOOL / TOBI OETIKER

Monitor Event Sources

NIDS Monitoring (Cisco IPS examples)

```
ids-1# show version
Application Partition:

Cisco Intrusion Prevention System, Version 6.1(1)E2

-- output clipped for brevity --

MainApp          M-2008_APR_24_19_16    (Release)   2008-04-24T19:49:05-0500   Running
AnalysisEngine   ME-2008_JUN_05_18_26   (Release)   2008-06-05T18:55:02-0500   Running
CLI              M-2008_APR_24_19_16    (Release)   2008-04-24T19:49:05-0500
-- output clipped for brevity --
```

Ensure key processes are running

```
ids-1# show version
Application Partition:

Cisco Intrusion Prevention System, Version 6.1(1)E2

-- output clipped for brevity --

Using 1901985792 out of 4100345856 bytes of available memory (46% usage)
system is using 17.7M out of 29.0M bytes of available disk space (61% usage)
application-data is using 51.6M out of 166.8M bytes of available disk space (33% usage)
boot is using 40.6M out of 69.5M bytes of available disk space (62% usage)

-- output clipped for brevity --
```

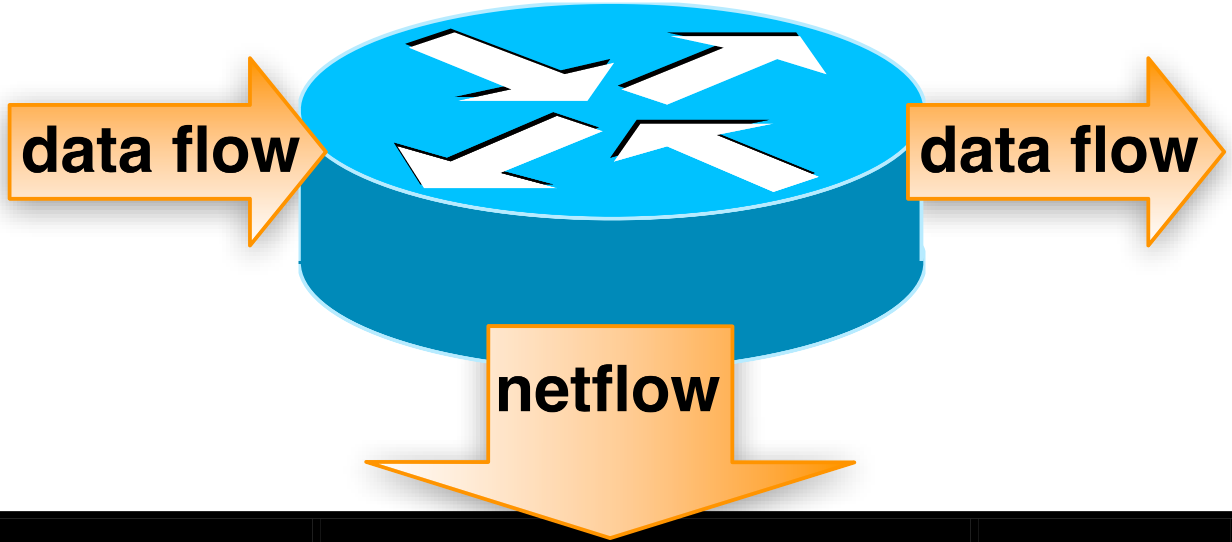
Monitor available memory

Monitor Event Sources

NetFlow

- Telemetry pushed from Cisco devices
  - Simple summary of connections
  - Negligible performance impact on routers
- Supported by Juniper & Alcatel (cflowd), Huawei (NetStream)
- Free!
- Like a phone bill
  - Packet capture is like a wire tap

- Used for IR, investigations, anomaly detection
- Collection tools
  - Some offer compression
  - OSU Flow Tools (free)
  - nfdump (free)
  - Cisco NetFlow Collector

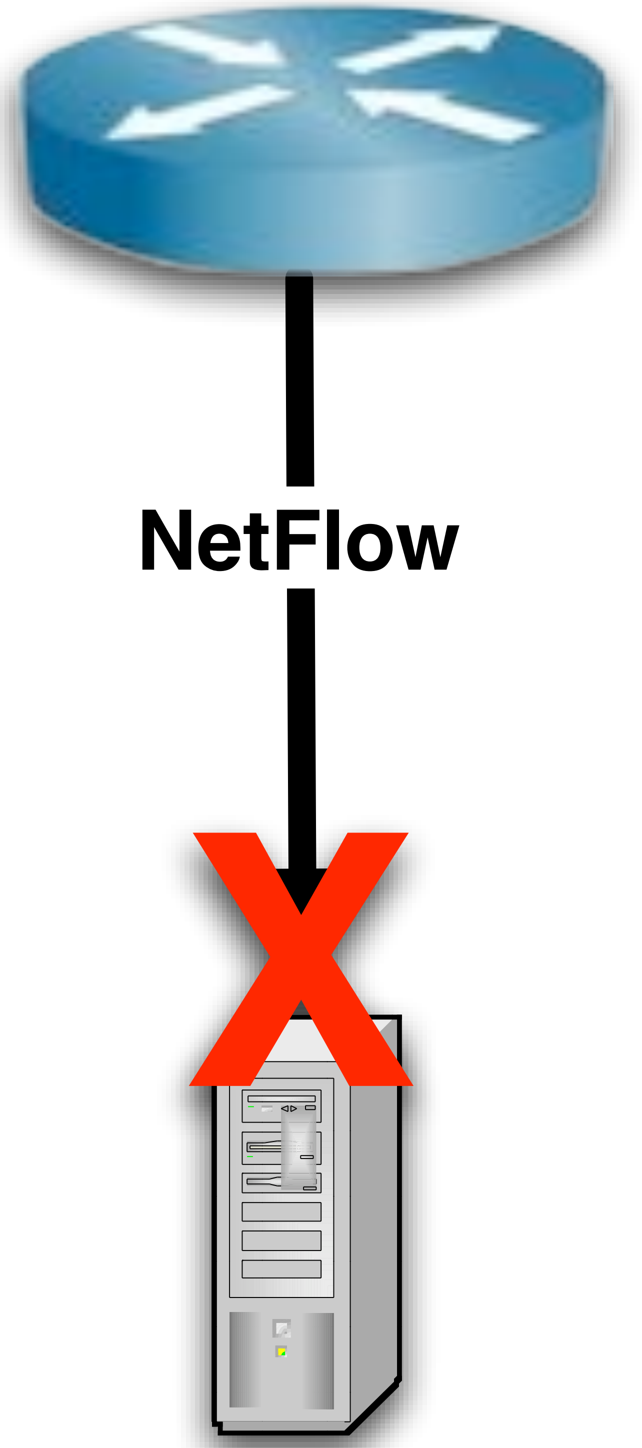


Source IP:Port	Destination IP:Port	Packets	Date/Time
192.168.15.7:2068	211.160.17.195:8080	7	5/7/2008 8:11:13 GMT
192.168.21.5:1042	72.18.45.223:21	219	5/7/2008 9:00:03 GMT
192.168.6.22:3161	172.18.15.188:80	1	5/7/2008 9:05:16 GMT

Monitor Event Sources

NetFlow Collection - Common Problems

- Flow exports changed/ removed
- Network changes prevent flows from reaching collector
- Capture process stops running
- File systems:
  - Not mounted or writable
  - Full



NetFlow collector

Monitor Event Sources

NetFlow Monitoring - Manual Checks

Ensure collector listening for NetFlow

```
[mnystrom@blanco-dc-nfc-1 ~]$ netstat -l | grep 2055
udp        0      0 *:2055                      *:*
```

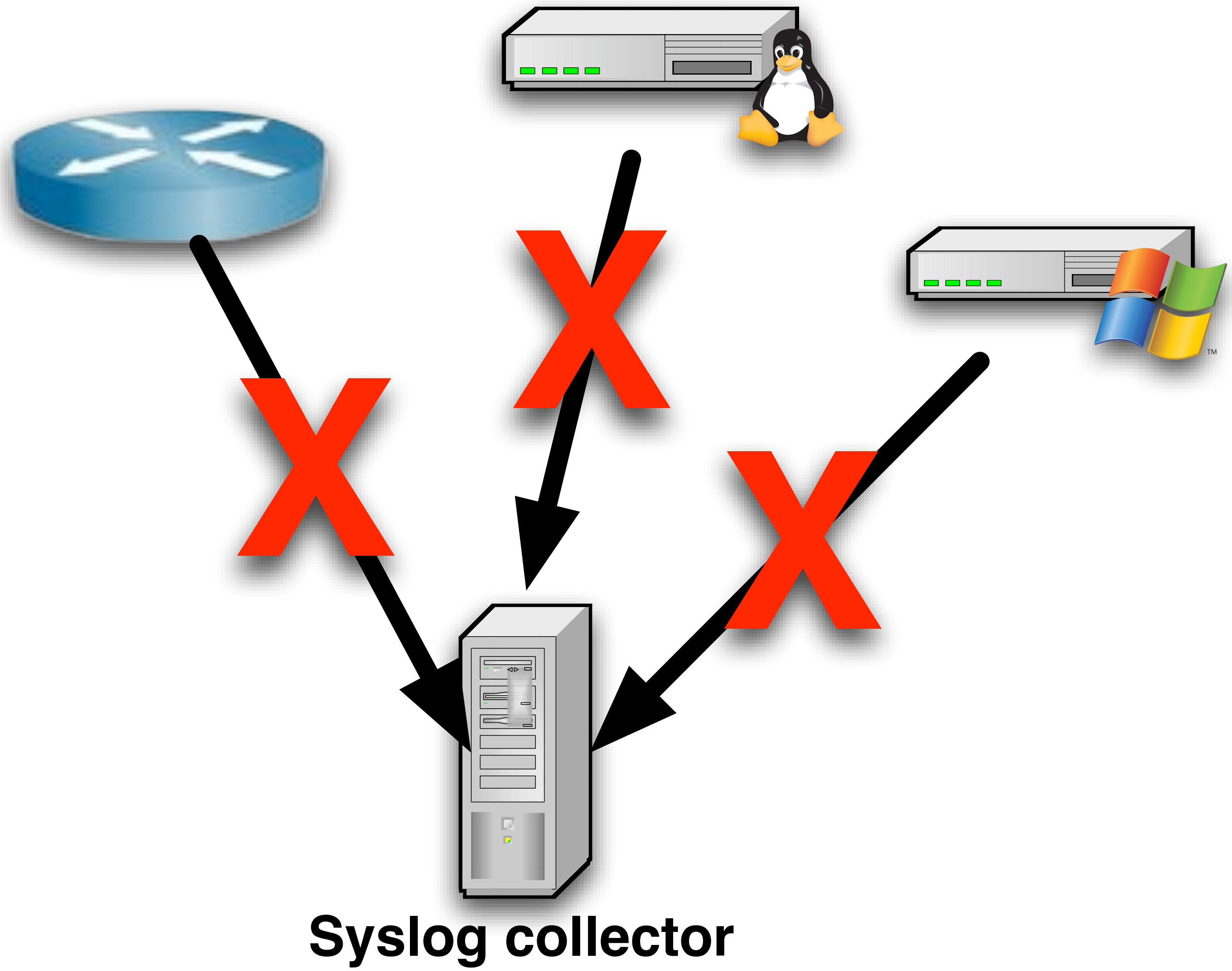
Ensure router sending NetFlow to collector

```
dc-gw1>show ip flow export
Flow export v5 is enabled for main cache
  Exporting flows to 10.83.4.99 (2055)
  Exporting using source interface Loopback0
  Version 5 flow records, peer-as
  327844689 flows exported in 10928453 udp datagrams
  0 flows failed due to lack of export packet
  1 export packets were sent up to process level
  4 export packets were dropped due to no fib
  4 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
  0 export packets were dropped enqueuing for the RP
  0 export packets were dropped due to IPC rate limiting
```

Source Types

Host and Device Logs - Common Problems

- Devices not exporting to collector
- Not exporting correct event types
- Collector not listening
- File systems:
  - Not mounted or writable
  - Full



Monitor Event Sources

Host and Device Monitoring -- Manual Checks

Monitor configs to ensure sending events

```
$ ssh webserver-1 grep 10.83.4.102 /etc/syslog.conf
*.*                                          @10.83.4.102
```

Monitor log configuration

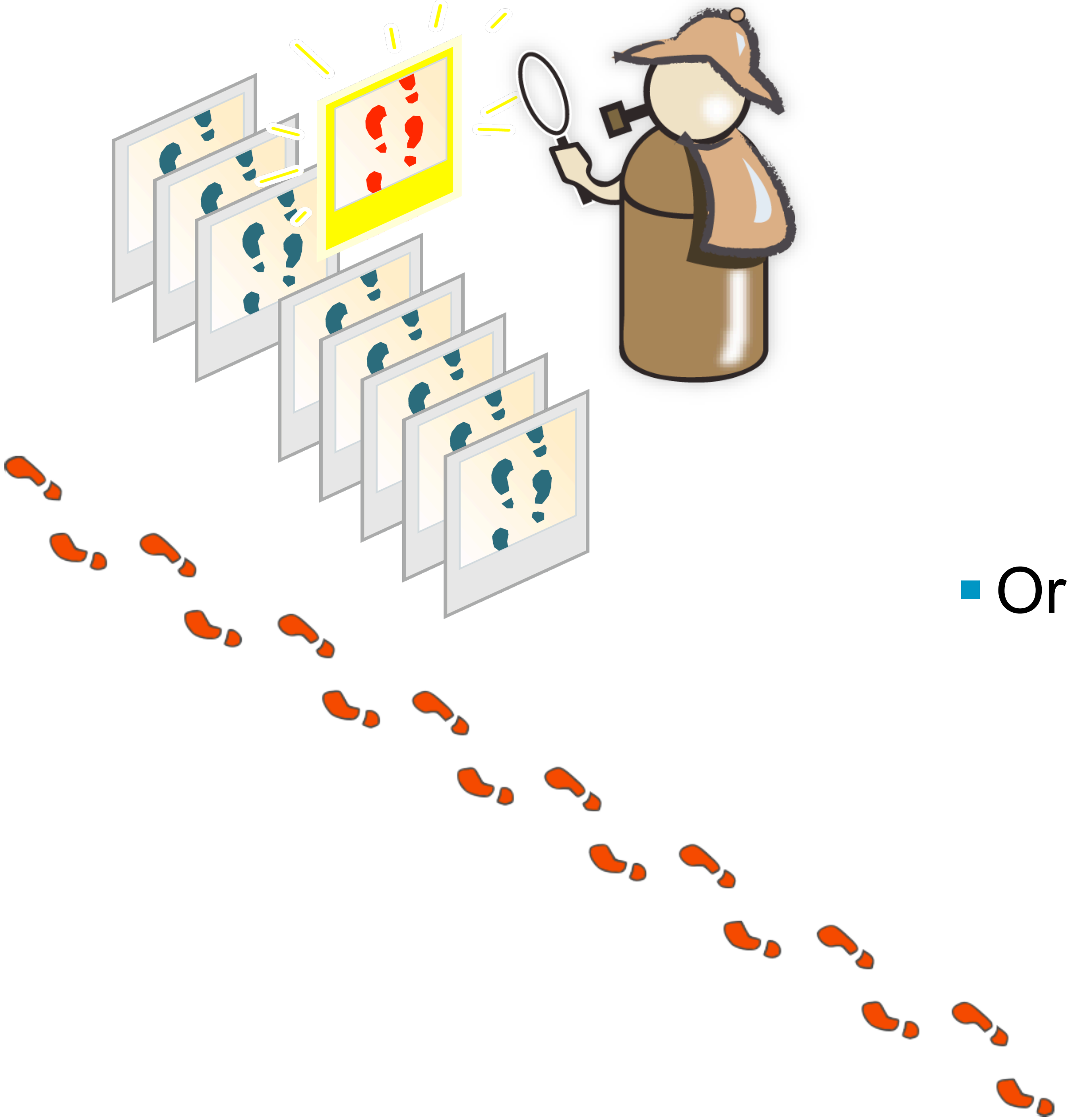
Check for recent events from each device

```
[mnystrom@collector-1 logs]$ egrep "Sep 19 03:.*webserver-1" /apps/logs/all-*
/apps/logs/all-06:Sep 19 03:27:35 webserver-1 ntpdate[9910]: [ID 558275
daemon.notice] adjust time server 10.81.254.202 offset 0.037428 sec

/apps/logs/all-06:Sep 19 03:30:22 webserver-1 sshd[9967]: [ID 800047
local3.info] Accepted rsa for root from 171.70.170.241 port 45915
```

Monitor incoming events

Monitor Event Sources

Web Server and Database Logs

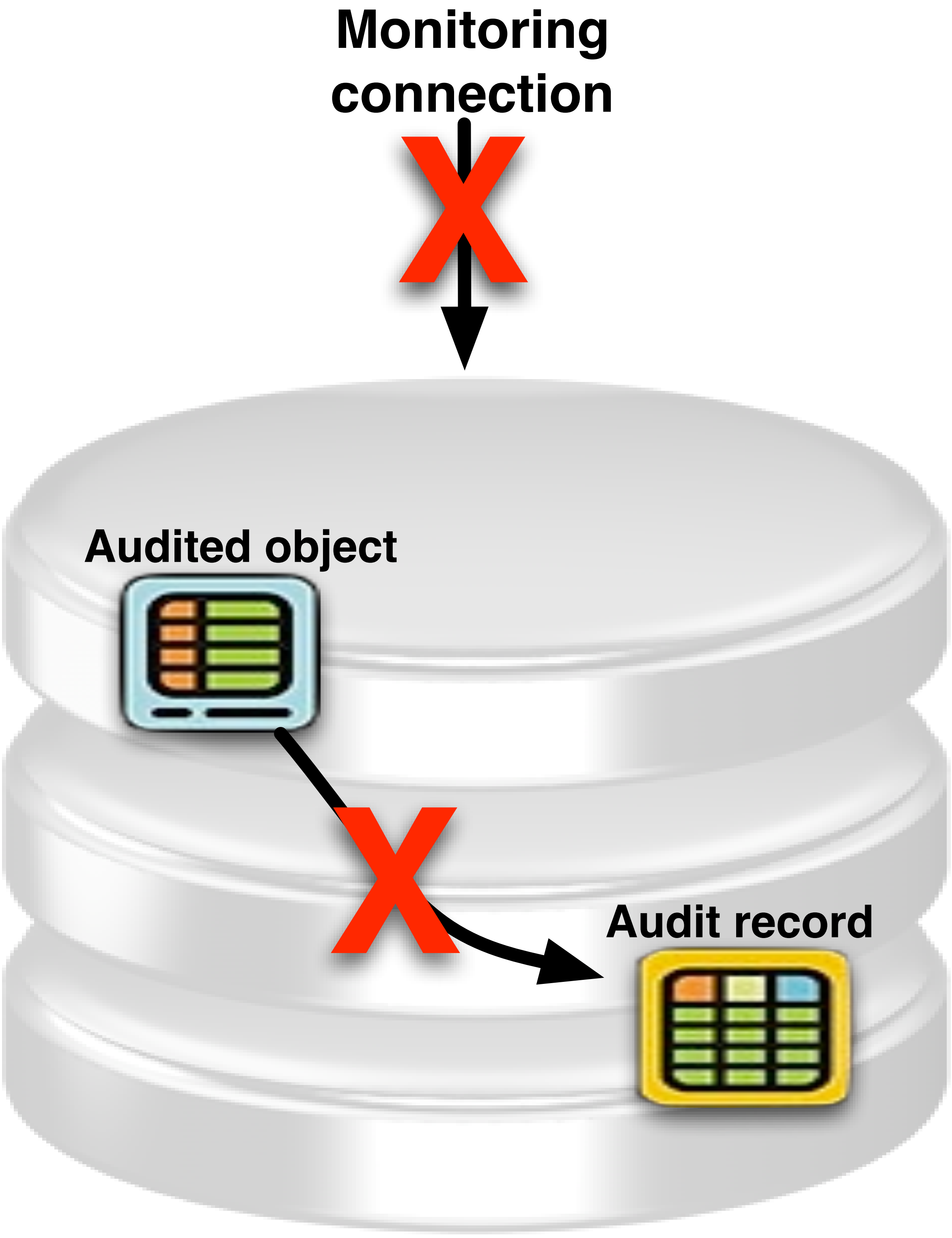


- Web server logs
  - Can verify and elucidate attacks
    - Use HTTP status codes to determine if IDS alert really worked
    - Provide URL details used in attack
  - Capturing...
    - **Apache**: Send as syslog via httpd.conf setting
    - **IIS**: Send as syslog via MonitorWare Agent
- Oracle logs
  - Pull logs from AUD$ table via SQL
  - Types of auditing
    - Statement
    - Fine-grained (FGA)
    - Privilege
    - Schema object

Monitor Event Sources

Database Logs -- Common Problems

- Broken connection
  - Network errors
  - Database errors
  - Account/password problems
- Auditing disabled
  - Events no longer being recorded



Monitor Event Sources

Database Events -- Manual Checks

Ensure connectivity to retrieve events

```
thor$ sqlplus watchdog/tiger@dbprod

Connected to dbprod as watchdog from thor
Your sessionid is 313854
Oracle8i Enterprise Edition Release 8.1.7.3.0 - Production
```

```
select count(*) from SYS.AUD$ where
(current_timestamp - aud$.timestamp#) > 5*1/24/60

count(*)
--------
0
```

Check for recent events:
No events logged in past 5 minutes

System Monitoring Solutions

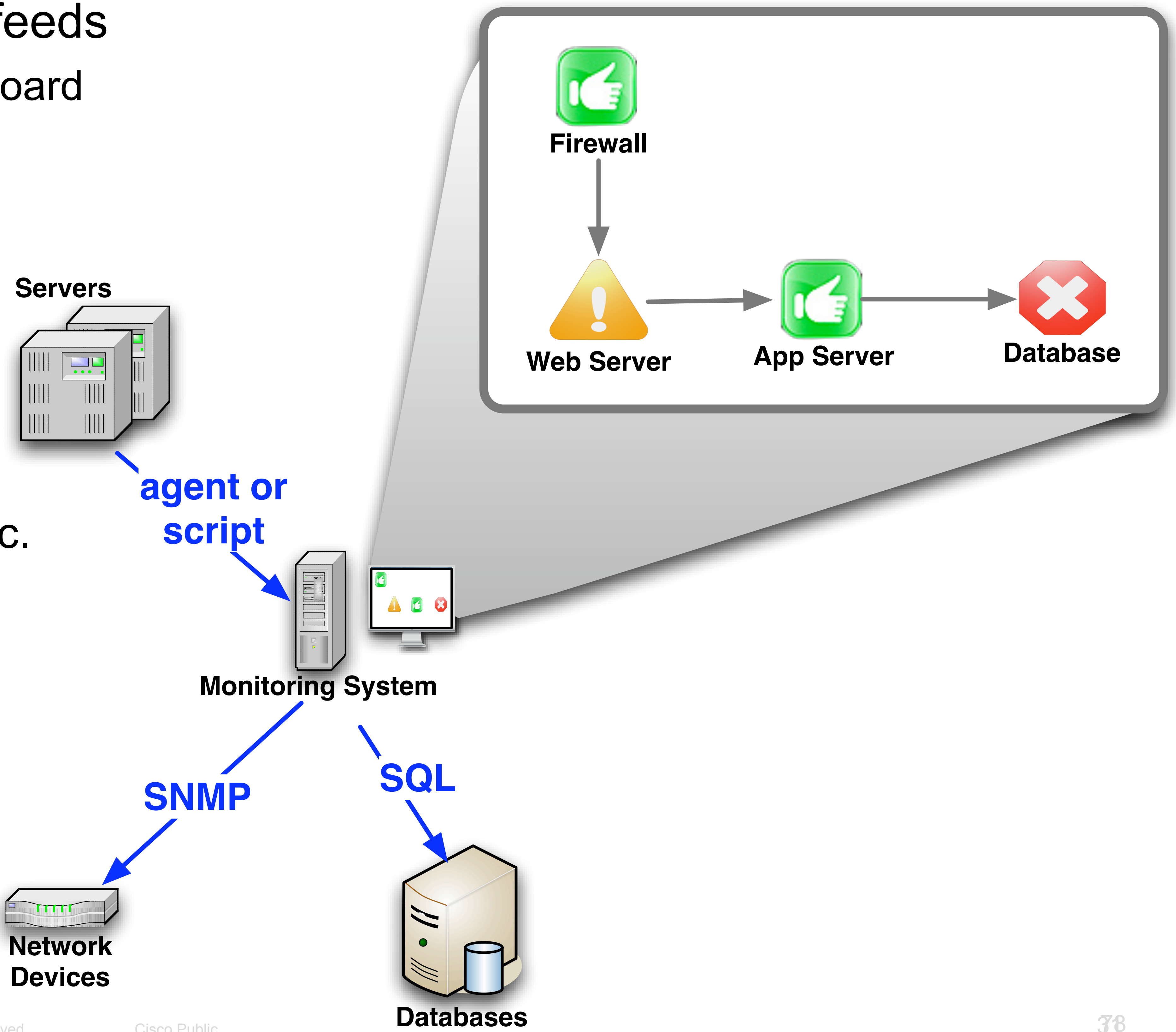
System Monitoring Solutions

Need for Automation

- Problems with manual checks
  - Not scalable
  - Unreliable (ad-hoc)
  - Inefficient
  - No metrics
- Packaged systems
  - Traditionally for network availability monitoring
  - Commercial examples: HP OpenView, Tivoli, CA Unicenter
  - Open source examples: OpenNMS, Pandora FMS, Zenoss, Nagios

System Monitoring Solutions
Overview

- Use tools to monitor feeds
  - Shows status in dashboard
  - Can script fixes
    - *restarts, etc.*
- Watches
  - Health of hosts
  - Volume of logs/traffic
- Scriptable
  - Shell, Perl, Expect, etc.



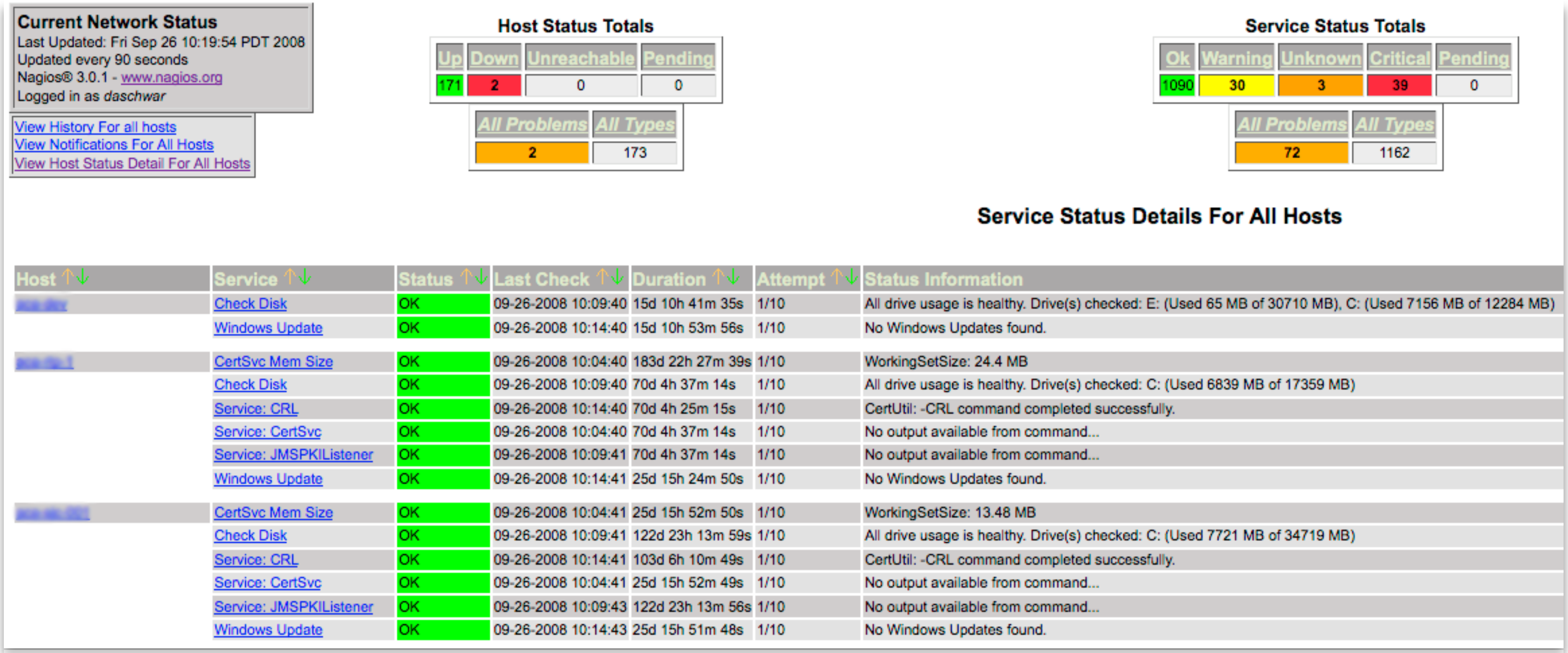
System Monitoring Solutions

Nagios®

Copyright (c) 1999-2008 Ethan Galstad

- Open source system monitoring solution
- Automated health monitoring of security events

- Simple to deploy
- Flexible and easily extensible
- GNU GPL 2 License



Current Network Status
Last Updated: Fri Sep 26 10:19:54 PDT 2008
Updated every 90 seconds
Nagios® 3.0.1 - www.nagios.org
Logged in as *daschwar*

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
171	2	0	0

All Problems	All Types
2	173

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
1090	30	3	39	0

All Problems	All Types
72	1162

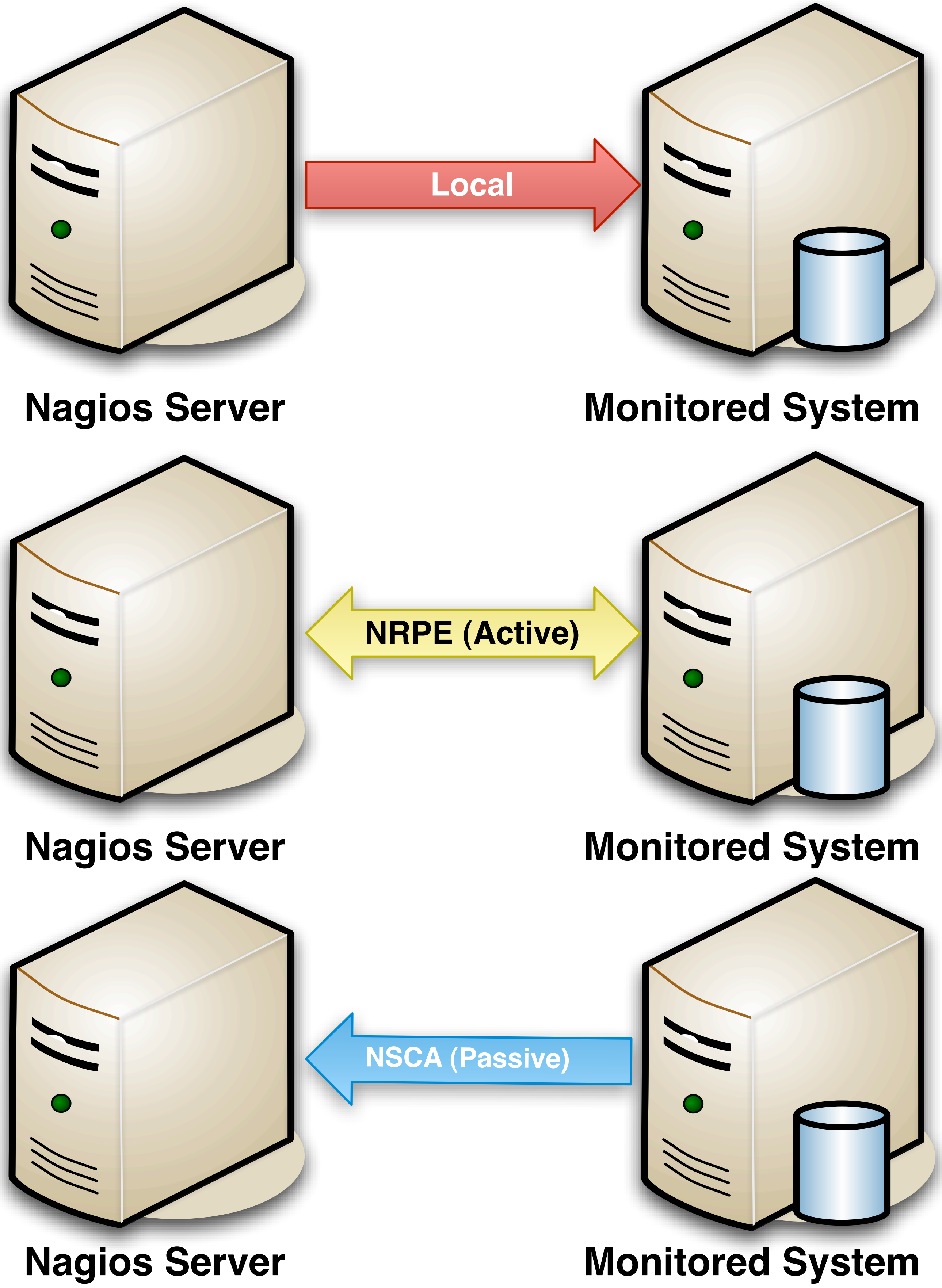
Service Status Details For All Hosts

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
[redacted]	Check Disk	OK	09-26-2008 10:09:40	15d 10h 41m 35s	1/10	All drive usage is healthy. Drive(s) checked: E: (Used 65 MB of 30710 MB), C: (Used 7156 MB of 12284 MB)
	Windows Update	OK	09-26-2008 10:14:40	15d 10h 53m 56s	1/10	No Windows Updates found.
[redacted]	CertSvc Mem Size	OK	09-26-2008 10:04:40	183d 22h 27m 39s	1/10	WorkingSetSize: 24.4 MB
	Check Disk	OK	09-26-2008 10:09:40	70d 4h 37m 14s	1/10	All drive usage is healthy. Drive(s) checked: C: (Used 6839 MB of 17359 MB)
	Service: CRL	OK	09-26-2008 10:14:40	70d 4h 25m 15s	1/10	CertUtil: -CRL command completed successfully.
	Service: CertSvc	OK	09-26-2008 10:04:40	70d 4h 37m 14s	1/10	No output available from command...
	Service: JMSPKIListener	OK	09-26-2008 10:09:41	70d 4h 37m 14s	1/10	No output available from command...
	Windows Update	OK	09-26-2008 10:14:41	25d 15h 24m 50s	1/10	No Windows Updates found.
[redacted]	CertSvc Mem Size	OK	09-26-2008 10:04:41	25d 15h 52m 50s	1/10	WorkingSetSize: 13.48 MB
	Check Disk	OK	09-26-2008 10:09:41	122d 23h 13m 59s	1/10	All drive usage is healthy. Drive(s) checked: C: (Used 7721 MB of 34719 MB)
	Service: CRL	OK	09-26-2008 10:14:41	103d 6h 10m 49s	1/10	CertUtil: -CRL command completed successfully.
	Service: CertSvc	OK	09-26-2008 10:04:41	25d 15h 52m 49s	1/10	No output available from command...
	Service: JMSPKIListener	OK	09-26-2008 10:09:43	122d 23h 13m 56s	1/10	No output available from command...
	Windows Update	OK	09-26-2008 10:14:43	25d 15h 51m 48s	1/10	No Windows Updates found.

System Monitoring Solutions

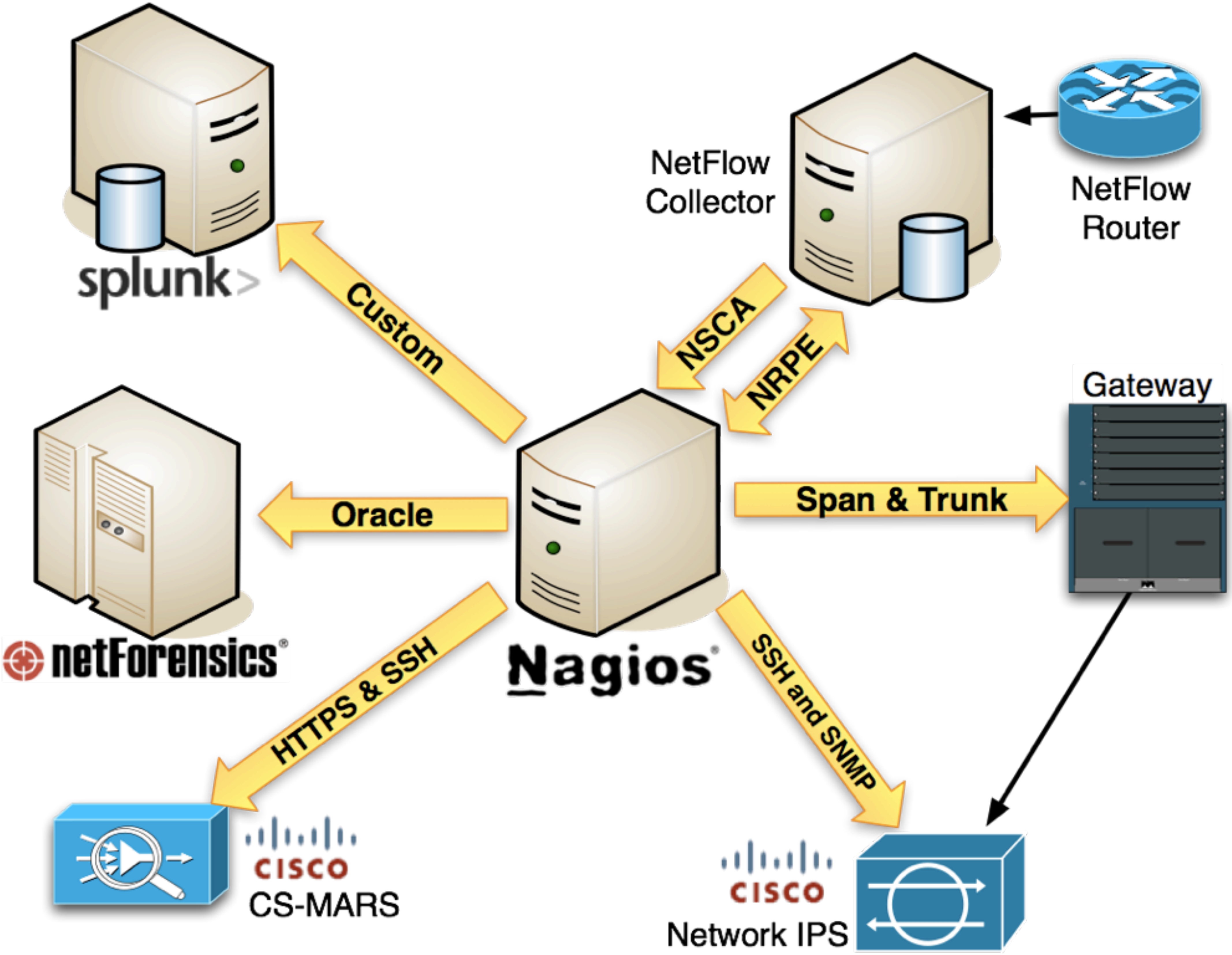
How Nagios Works

- Server local checks
  - HTTP(S)
  - Ping
  - SNMP
  - Telnet/SSH
  - And more...
- Remote checks
  - NRPE (active)
    - Server triggers check
  - NSCA (passive)
    - Client reports results to server



System Monitoring Solutions

How Cisco CSIRT Uses Nagios

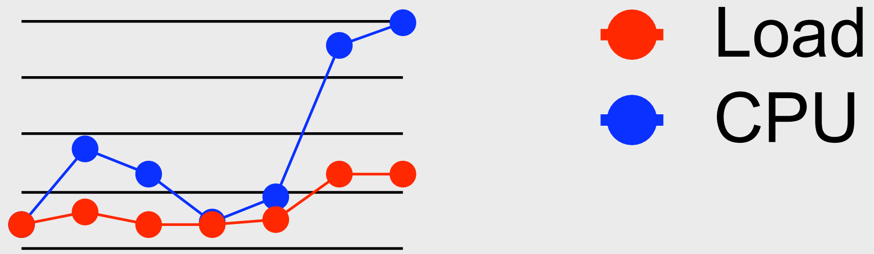


System Monitoring Solutions

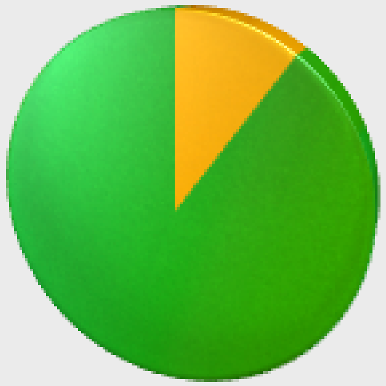
Health Monitoring

Connectivity to Host

System Load



Memory



Monitor both:

- **Physical memory**
- **Swap**

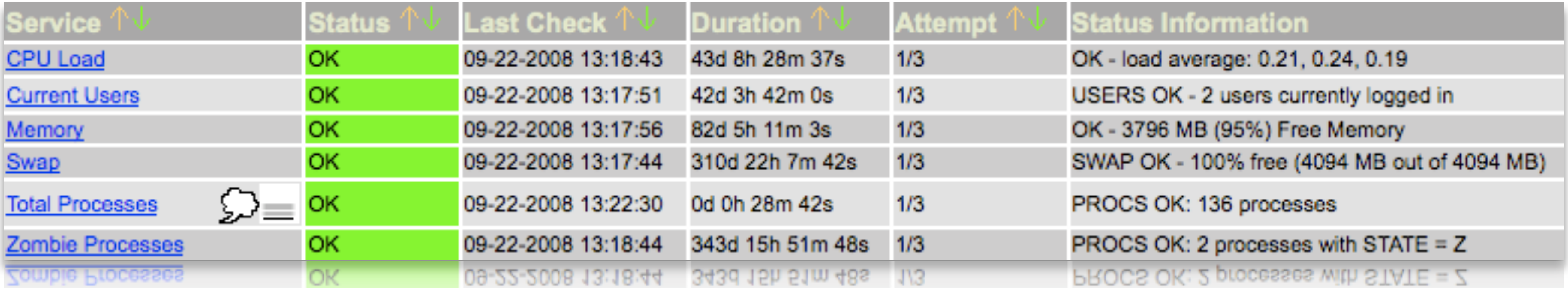
Disk Space

Processes

● Total
● Zombie

System Monitoring Solutions

System Health: Nagios Monitoring



Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
CPU Load	OK	09-22-2008 13:18:43	43d 8h 28m 37s	1/3	OK - load average: 0.21, 0.24, 0.19
Current Users	OK	09-22-2008 13:17:51	42d 3h 42m 0s	1/3	USERS OK - 2 users currently logged in
Memory	OK	09-22-2008 13:17:56	82d 5h 11m 3s	1/3	OK - 3796 MB (95%) Free Memory
Swap	OK	09-22-2008 13:17:44	310d 22h 7m 42s	1/3	SWAP OK - 100% free (4094 MB out of 4094 MB)
Total Processes	OK	09-22-2008 13:22:30	0d 0h 28m 42s	1/3	PROCS OK: 136 processes
Zombie Processes	OK	09-22-2008 13:18:44	343d 15h 51m 48s	1/3	PROCS OK: 2 processes with STATE = Z

- CPU Load
- Number of users
- Memory and swap
- Processes and zombies
- Disk health

System Monitoring Solutions

System Health

```
check_ping -H $HOSTADDRESS$ -w 3000.0,80% -c 5000.0,100% -p 1
```

Connectivity
Warn > 3000 ms
Critical > 5000 ms

```
check_load -w 15,10,5 -c 30,25,20
```

System load
Warn > 5,10,15
Critical > 20,25,30

Free memory
Warn < 5%
Critical < 1%

Free swap
Warn < 90%
Critical < 80%

```
check_mem -w 5 -c 1
```

```
check_swap -w 90%% -c 80%%
```

Disk space
Warn < 10%
Critical < 5%

```
check_disk -w 10 -c 5 -p /apps/data
```

System Monitoring Solutions

NIDS Monitoring

Span and Trunk Health

Routers configured to mirror traffic to NIDS?

dc-gw-1	🔴
dc-gw-3	🔴

Alerts Logged

Monitor for recent alerts logged to SIM

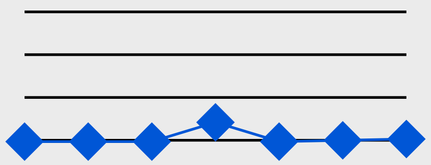
NIDS	Last Alert
NIDS-1	10 minutes ago
NIDS-2	43 minutes ago

Critical Processes

Monitor running processes

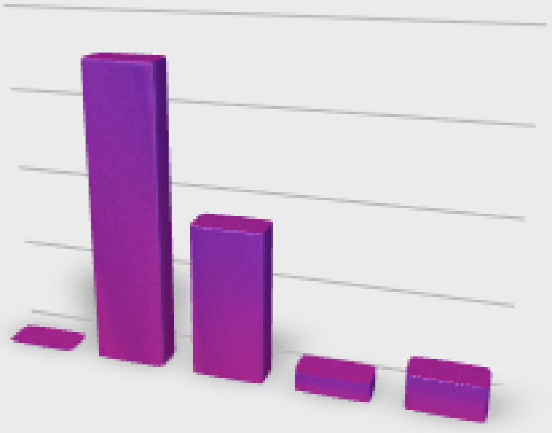
Analysis Engine	🔴
HTTPS	🟢

Missed Packets



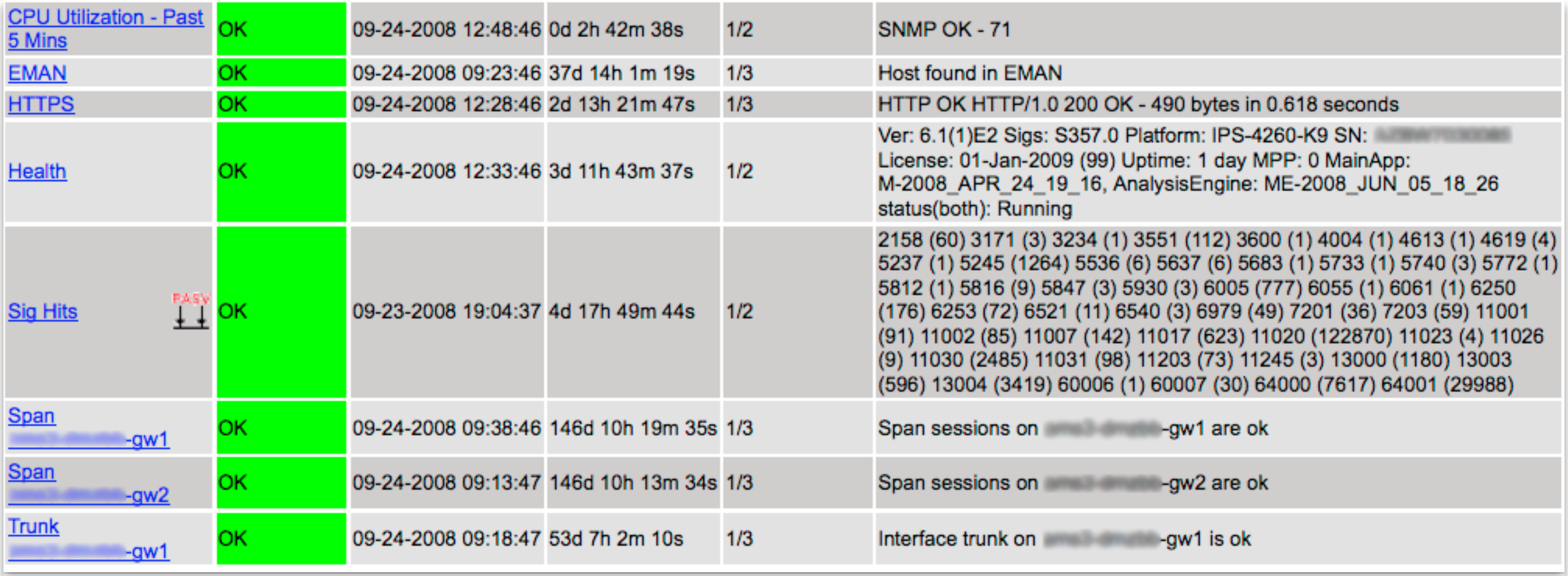
Top Signatures

Monitor hits to each signature



System Monitoring Solutions

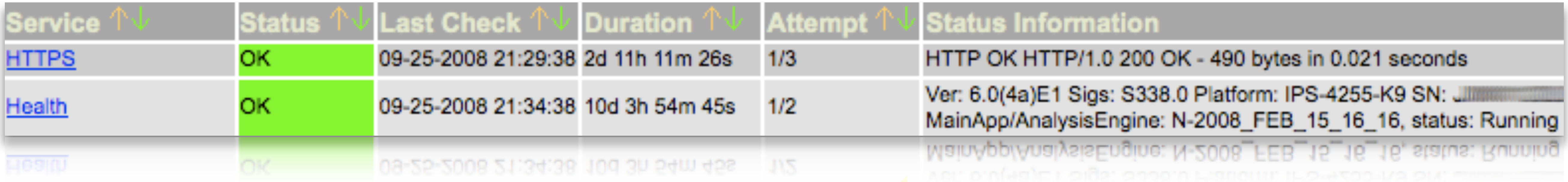
Network IDS: Nagios Monitoring



CPU Utilization - Past 5 Mins	OK	09-24-2008 12:48:46	0d 2h 42m 38s	1/2	SNMP OK - 71
EMAN	OK	09-24-2008 09:23:46	37d 14h 1m 19s	1/3	Host found in EMAN
HTTPS	OK	09-24-2008 12:28:46	2d 13h 21m 47s	1/3	HTTP OK HTTP/1.0 200 OK - 490 bytes in 0.618 seconds
Health	OK	09-24-2008 12:33:46	3d 11h 43m 37s	1/2	Ver: 6.1(1)E2 Sigs: S357.0 Platform: IPS-4260-K9 SN: [redacted] License: 01-Jan-2009 (99) Uptime: 1 day MPP: 0 MainApp: M-2008_APR_24_19_16, AnalysisEngine: ME-2008_JUN_05_18_26 status(both): Running
Sig Hits PASV	OK	09-23-2008 19:04:37	4d 17h 49m 44s	1/2	2158 (60) 3171 (3) 3234 (1) 3551 (112) 3600 (1) 4004 (1) 4613 (1) 4619 (4) 5237 (1) 5245 (1264) 5536 (6) 5637 (6) 5683 (1) 5733 (1) 5740 (3) 5772 (1) 5812 (1) 5816 (9) 5847 (3) 5930 (3) 6005 (777) 6055 (1) 6061 (1) 6250 (176) 6253 (72) 6521 (11) 6540 (3) 6979 (49) 7201 (36) 7203 (59) 11001 (91) 11002 (85) 11007 (142) 11017 (623) 11020 (122870) 11023 (4) 11026 (9) 11030 (2485) 11031 (98) 11203 (73) 11245 (3) 13000 (1180) 13003 (596) 13004 (3419) 60006 (1) 60007 (30) 64000 (7617) 64001 (29988)
Span [redacted]-gw1	OK	09-24-2008 09:38:46	146d 10h 19m 35s	1/3	Span sessions on [redacted]-gw1 are ok
Span [redacted]-gw2	OK	09-24-2008 09:13:47	146d 10h 13m 34s	1/3	Span sessions on [redacted]-gw2 are ok
Trunk [redacted]-gw1	OK	09-24-2008 09:18:47	53d 7h 2m 10s	1/3	Interface trunk on [redacted]-gw1 is ok

System Monitoring Solutions

Network IDS: Critical Processes



Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
HTTPS	OK	09-25-2008 21:29:38	2d 11h 11m 26s	1/3	HTTP OK HTTP/1.0 200 OK - 490 bytes in 0.021 seconds
Health	OK	09-25-2008 21:34:38	10d 3h 54m 45s	1/2	Ver: 6.0(4a)E1 Sigs: S338.0 Platform: IPS-4255-K9 SN: [redacted] MainApp/AnalysisEngine: N-2008_FEB_15_16_16, status: Running

```
check_http --ssl -H $HOSTADDRESS$
```

HTTPS

Ensure web interface is accessible

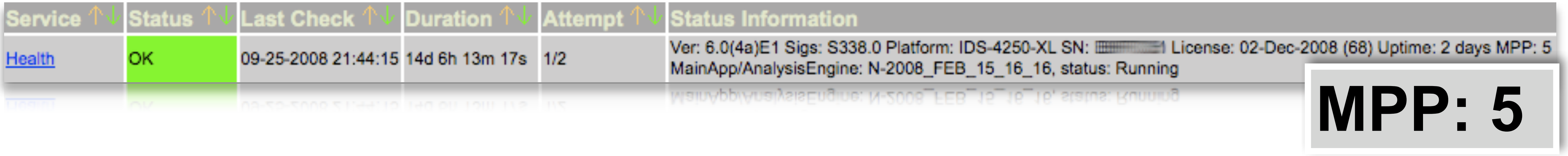
```
nids-1# show version
Application Partition:

Cisco Intrusion Prevention System, Version
6.1(1)E2
...
MainApp           M-2008_APR_24_19_16
(Release)     2008-04-24T19:49:05-0500    Running
AnalysisEngine    ME-2008_JUN_05_18_26
(Release)     2008-06-05T18:55:02-0500    Running
```

Expect script via SSH

Critical alert if "Running" not found after AnalysisEngine

System Monitoring Solutions

Network IDS: Missed Packets



Service	Status	Last Check	Duration	Attempt	Status Information
Health	OK	09-25-2008 21:44:15	14d 6h 13m 17s	1/2	Ver: 6.0(4a)E1 Sigs: S338.0 Platform: IDS-4250-XL SN: [redacted] License: 02-Dec-2008 (68) Uptime: 2 days MPP: 5 MainApp/AnalysisEngine: N-2008_FEB_15_16_16, status: Running

MPP: 5

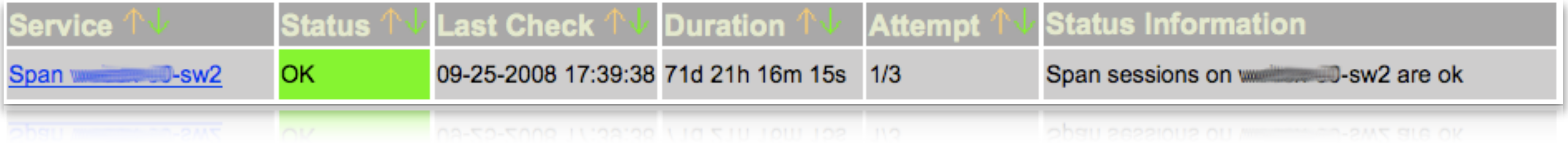
```
# show interface  GigabitEthernet2/1
MAC statistics from interface
GigabitEthernet2/1
   Interface function = Sensing interface
   Description =
-- output clipped for brevity
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Missed Packet Percentage = 5
   Total Packets Received = 7073135664
   Total Bytes Received = 4128666779156
   Total Multicast Packets Received = 7008095
```

Expect script via SSH

Report % missed packets for monitoring context

System Monitoring Solutions

Network IDS: Span Health on Routers



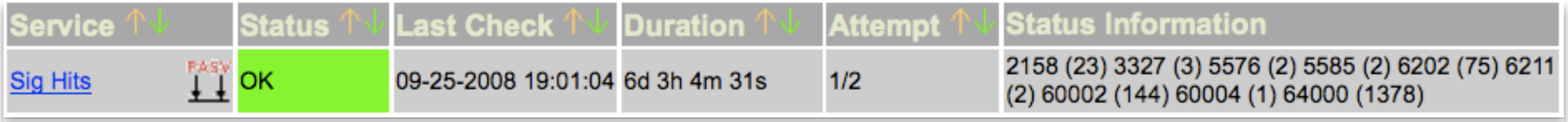
Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
Span [redacted]-sw2	OK	09-25-2008 17:39:38	71d 21h 16m 15s	1/3	Span sessions on [redacted]-sw2 are ok

```
blanco-gw1>show monitor session all
Session 1
---------
Type                    : Local Session
Source Ports            :
   Both               : Gi1/1
Destination Ports       : Gi3/11


Session 2
---------
Type                    : Local Session
Source Ports            :
   Both               : Gi1/2
Destination Ports       : Gi3/12
```

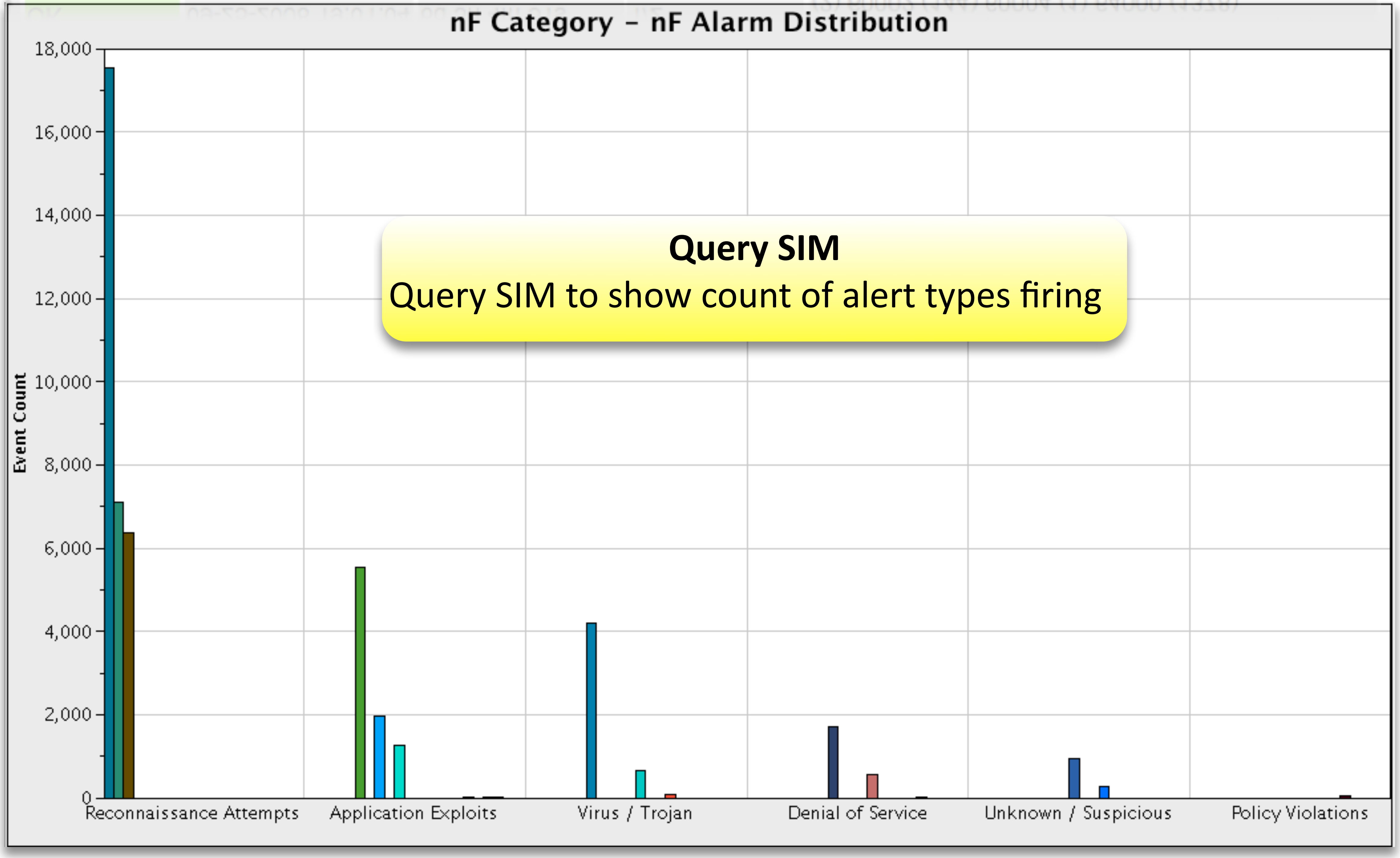
Perl script via SSH
Critical alert if output differs from expected output (diff comparison of previously saved output)

System Monitoring Solutions

Network IDS: Signatures Firing



Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
Sig Hits	OK	09-25-2008 19:01:04	6d 3h 4m 31s	1/2	2158 (23) 3327 (3) 5576 (2) 5585 (2) 6202 (75) 6211 (2) 60002 (144) 60004 (1) 64000 (1378)



Query SIM

Query SIM to show count of alert types firing

System Monitoring Solutions

NetFlow Monitoring

Processes

Monitor capture/relay processes running

flow-capture	🟡
flow-fanout	🟢

File System

Readable	🟢
Writeable	🔴

Maintain permissions for collection

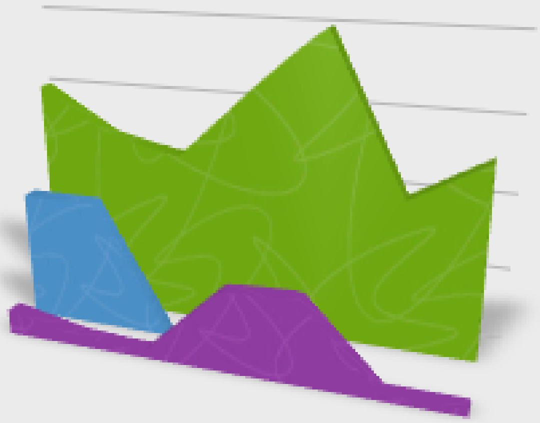
Data Files

Monitor data files written for each source

Log Dir	Last Write
/logs/server1	10 minutes ago
/logs/server2	43 minutes ago

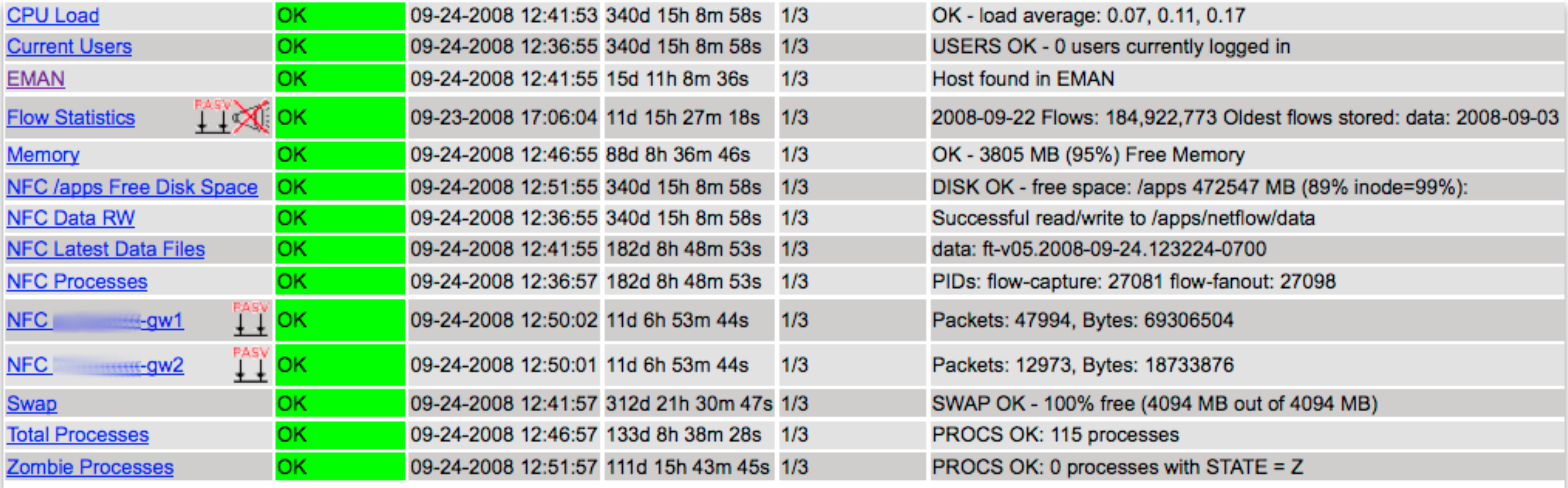
Traffic Volume

Monitor packets and bytes received from each source



System Monitoring Solutions

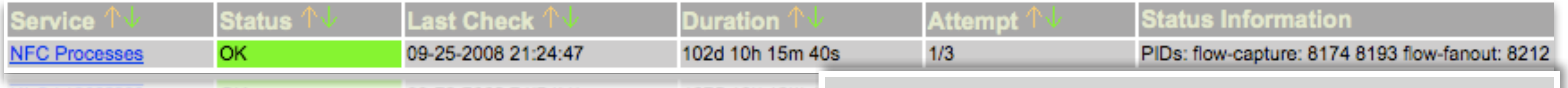
NetFlow Collection: Nagios Monitoring



CPU Load	OK	09-24-2008 12:41:53	340d 15h 8m 58s	1/3	OK - load average: 0.07, 0.11, 0.17
Current Users	OK	09-24-2008 12:36:55	340d 15h 8m 58s	1/3	USERS OK - 0 users currently logged in
EMAN	OK	09-24-2008 12:41:55	15d 11h 8m 36s	1/3	Host found in EMAN
Flow Statistics	OK	09-23-2008 17:06:04	11d 15h 27m 18s	1/3	2008-09-22 Flows: 184,922,773 Oldest flows stored: data: 2008-09-03
Memory	OK	09-24-2008 12:46:55	88d 8h 36m 46s	1/3	OK - 3805 MB (95%) Free Memory
NFC /apps Free Disk Space	OK	09-24-2008 12:51:55	340d 15h 8m 58s	1/3	DISK OK - free space: /apps 472547 MB (89% inode=99%):
NFC Data RW	OK	09-24-2008 12:36:55	340d 15h 8m 58s	1/3	Successful read/write to /apps/netflow/data
NFC Latest Data Files	OK	09-24-2008 12:41:55	182d 8h 48m 53s	1/3	data: ft-v05.2008-09-24.123224-0700
NFC Processes	OK	09-24-2008 12:36:57	182d 8h 48m 53s	1/3	PIDs: flow-capture: 27081 flow-fanout: 27098
NFC [redacted]-gw1	OK	09-24-2008 12:50:02	11d 6h 53m 44s	1/3	Packets: 47994, Bytes: 69306504
NFC [redacted]-gw2	OK	09-24-2008 12:50:01	11d 6h 53m 44s	1/3	Packets: 12973, Bytes: 18733876
Swap	OK	09-24-2008 12:41:57	312d 21h 30m 47s	1/3	SWAP OK - 100% free (4094 MB out of 4094 MB)
Total Processes	OK	09-24-2008 12:46:57	133d 8h 38m 28s	1/3	PROCS OK: 115 processes
Zombie Processes	OK	09-24-2008 12:51:57	111d 15h 43m 45s	1/3	PROCS OK: 0 processes with STATE = Z

System Monitoring Solutions

NetFlow: Check Processes



Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
NFC Processes	OK	09-25-2008 21:24:47	102d 10h 15m 40s	1/3	PIDs: flow-capture: 8174 8193 flow-fanout: 8212

flow-capture: 8174 8193

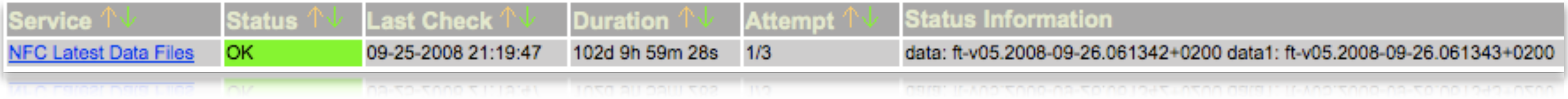
```
check_procs -c 3 -C flow-capture
```

Capture process

Critical alert if not 3 processes of *flow-capture*

System Monitoring Solutions

NetFlow: Data Files



Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
NFC Latest Data Files	OK	09-25-2008 21:19:47	102d 9h 59m 28s	1/3	data: ft-v05.2008-09-26.061342+0200 data1: ft-v05.2008-09-26.061343+0200

```
check_file_age  /apps/netflow/data
```

Check Latest Files

Plug-in has poor fidelity due to changing timestamps during cleanup

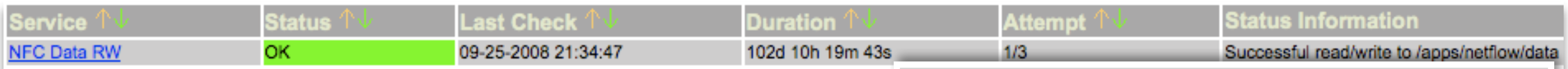
```
blanco-nfc#ls -l /apps/netflow/data/*
drwxr-xr-x    2 netflow infosec 12288 Sep 25 00:00 2008-09-24/
  -rw-r--r--  1 netflow infosec 82033098 Sep 25 11:22 ft-
  v05.2008-09-25.111738-0700
  -rw-r--r--  1 netflow infosec 73761724 Sep 25 11:27 ft-
  v05.2008-09-25.112238-0700
  -rw-r--r--  1 netflow infosec 74138352 Sep 25 11:32 ft-
  v05.2008-09-25.112737-0700
```

Custom Perl script via NRPE

Alert if not written within last 30 minutes

System Monitoring Solutions

NetFlow: File System



Service	Status	Last Check	Duration	Attempt	Status Information
NFC Data RW	OK	09-25-2008 21:34:47	102d 10h 19m 43s	1/3	Successful read/write to /apps/netflow/data

Successful read/write

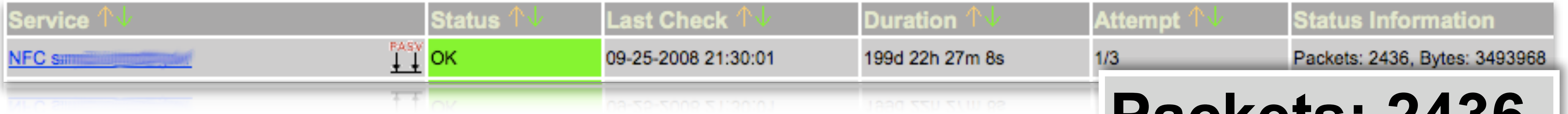
```
check_diskrw /apps/netflow/data
```

Check Permissions via NRPE

Alert if not *writeable*

System Monitoring Solutions

NetFlow: Traffic Volume



Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
NFC [redacted] PASV	OK	09-25-2008 21:30:01	199d 22h 27m 8s	1/3	Packets: 2436, Bytes: 3493968

Packets: 2436

```
[root@blanco-nfc ~]# iptables -vxL -Z INPUT
Chain INPUT (policy ACCEPT 9875 packets, 14M bytes)
 pkts bytes target     prot opt in     out     source
destination
   0     0     ACCEPT     udp  --  any     any      blanco-dc-gw1
   anywhere                udp dpt:2055
 2436 3412K ACCEPT     udp  --  any     any      blanco-dc-gw2
anywhere                udp dpt:2056
```

Check Received Traffic via iptables
Execute and send result via NSCA
Alert if packets not > 0 since last check

Implementation
Watch for New Event Sources

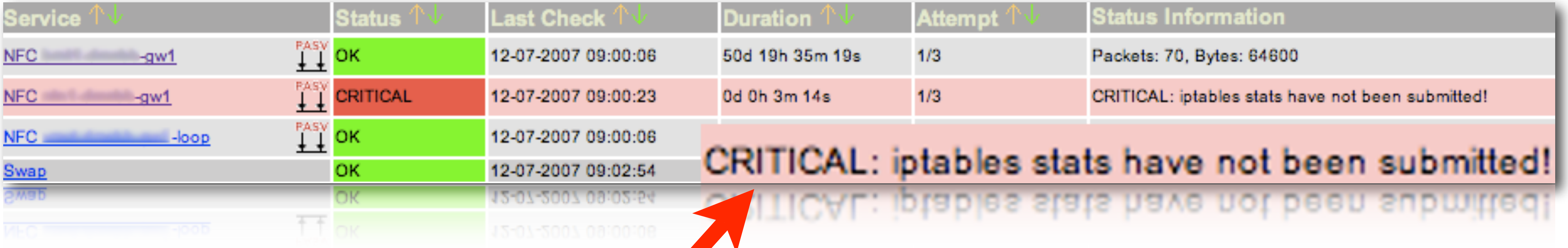
- Create policy
  - Require logging to your log collectors
  - Require specific events to log
  - Watch log collector for new hosts
  - Audit hosts to ensure compliance
- Watch for new devices
  - Change requests
  - IDS alerts
  - Network audits

Implementation
Checklist

1. Policy
2. SLAs
3. Templates
4. Config automation
5. Critical event sources
6. Monitoring package
7. Procedures
8. Training

Results

Benefits of Implementation



Service	Status	Last Check	Duration	Attempt	Status Information
NFC [redacted]-gw1	OK	12-07-2007 09:00:06	50d 19h 35m 19s	1/3	Packets: 70, Bytes: 64600
NFC [redacted]-gw1	CRITICAL	12-07-2007 09:00:23	0d 0h 3m 14s	1/3	CRITICAL: iptables stats have not been submitted!
NFC [redacted]-loop	OK	12-07-2007 09:00:06			
Swap	OK	12-07-2007 09:02:54			

CRITICAL: iptables stats have not been submitted!

- Real-time notification
- Programmable automation to resolve problems
- Result: Event metrics show improved up time
- At Cisco...
  - Before: < 90% (not tracked)
  - After: 97% and rising