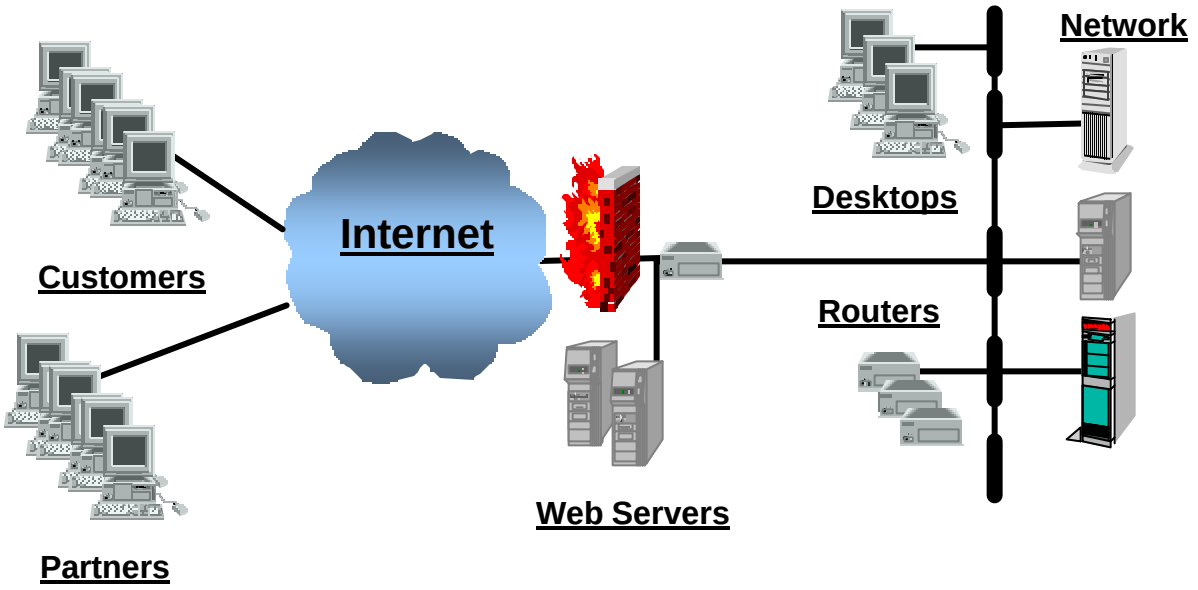
Deploying an Intrusion Detection Systems Solution for Internet Hosts

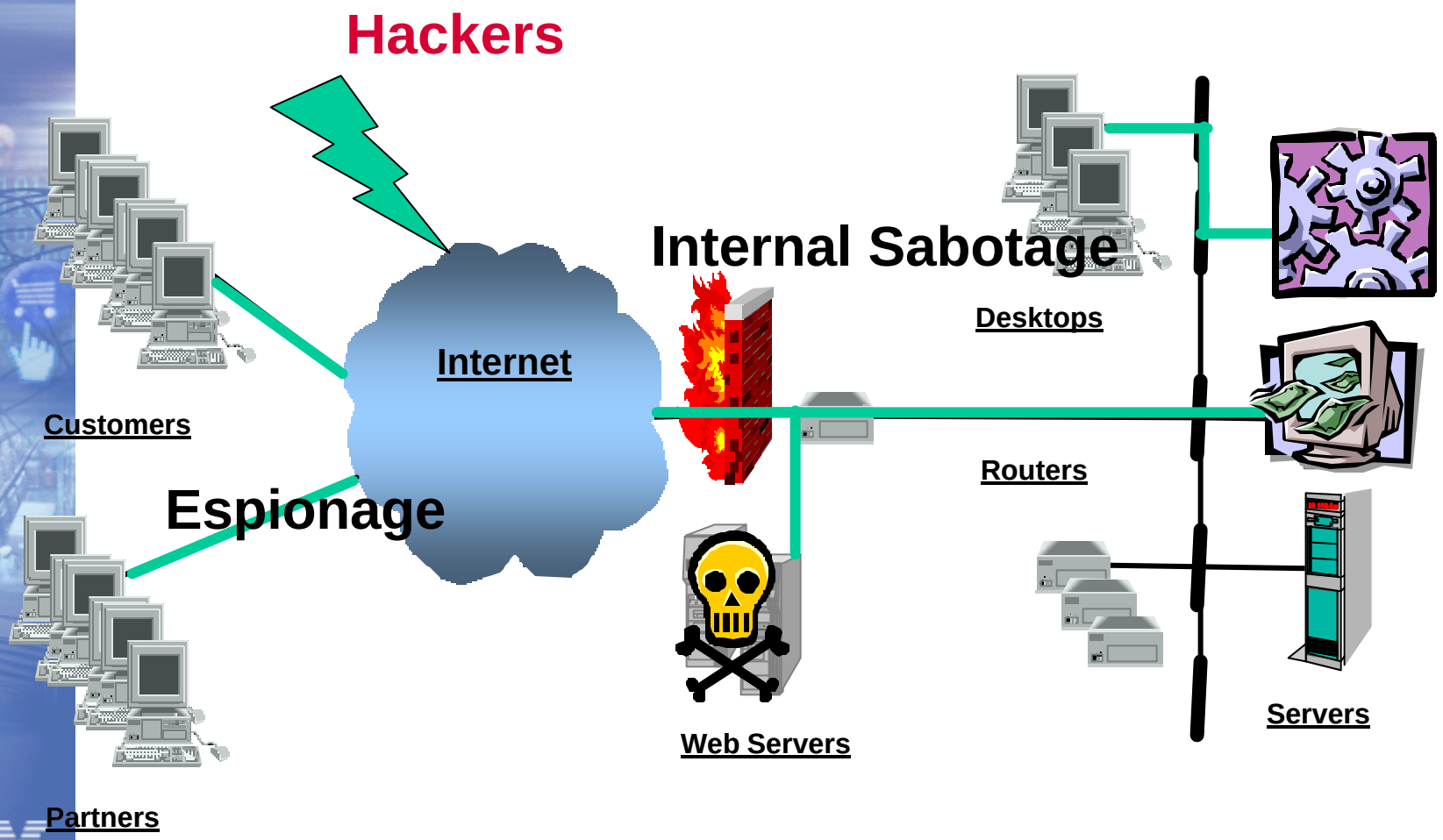
Douglas G. Conorich
Global Solutions Manager
Managed Security Services
IBM Global Services
conorich@us.ibm.com

The Business Problem

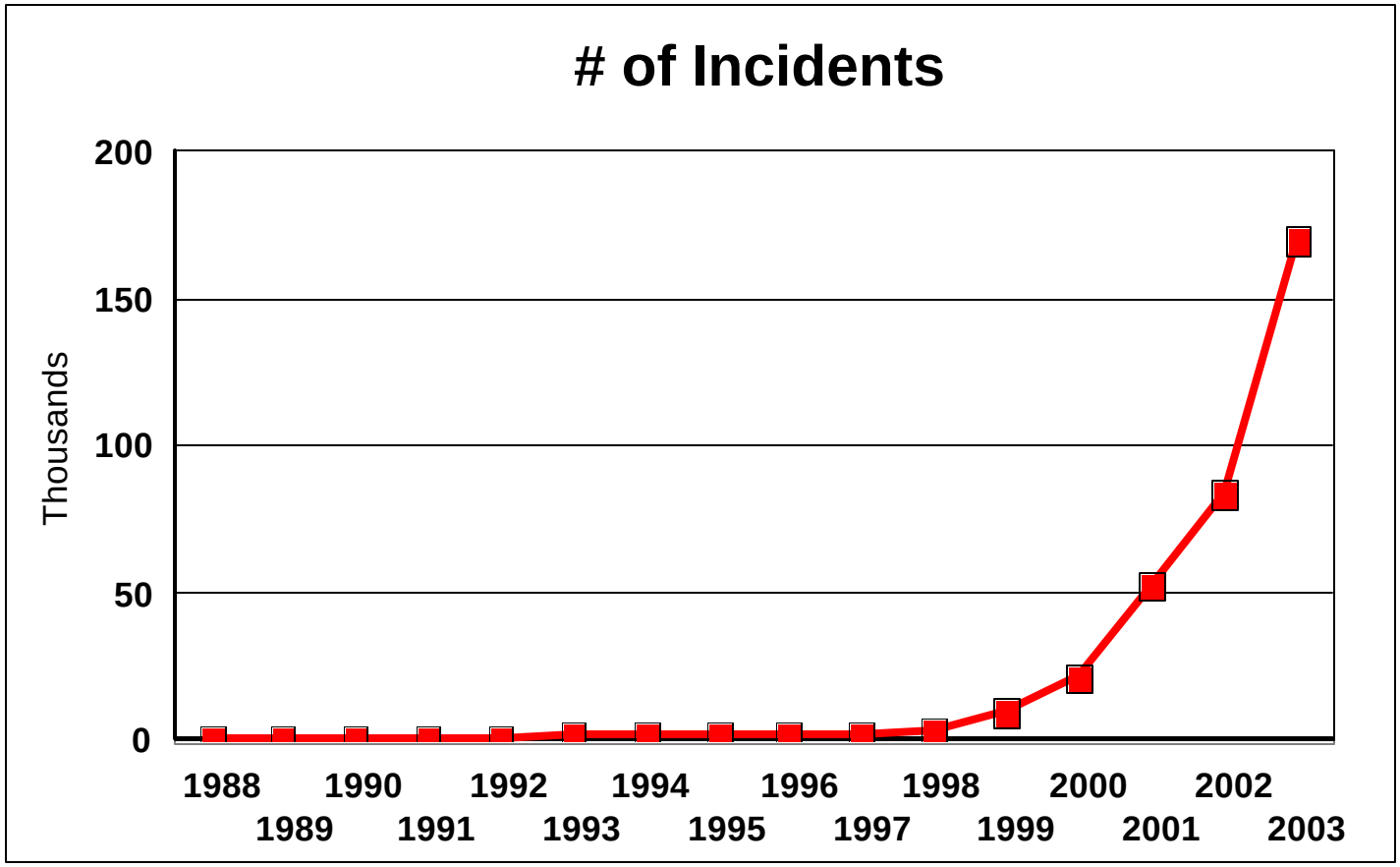
Companies need to open their networks to customers and suppliers while at the same time keeping hackers and malicious users out. However, security holes found in operating systems and applications along with a lack of security expertise often make it possible for the wrong users to access critical e-business systems, applications and data.



Multiple Points of Vulnerability

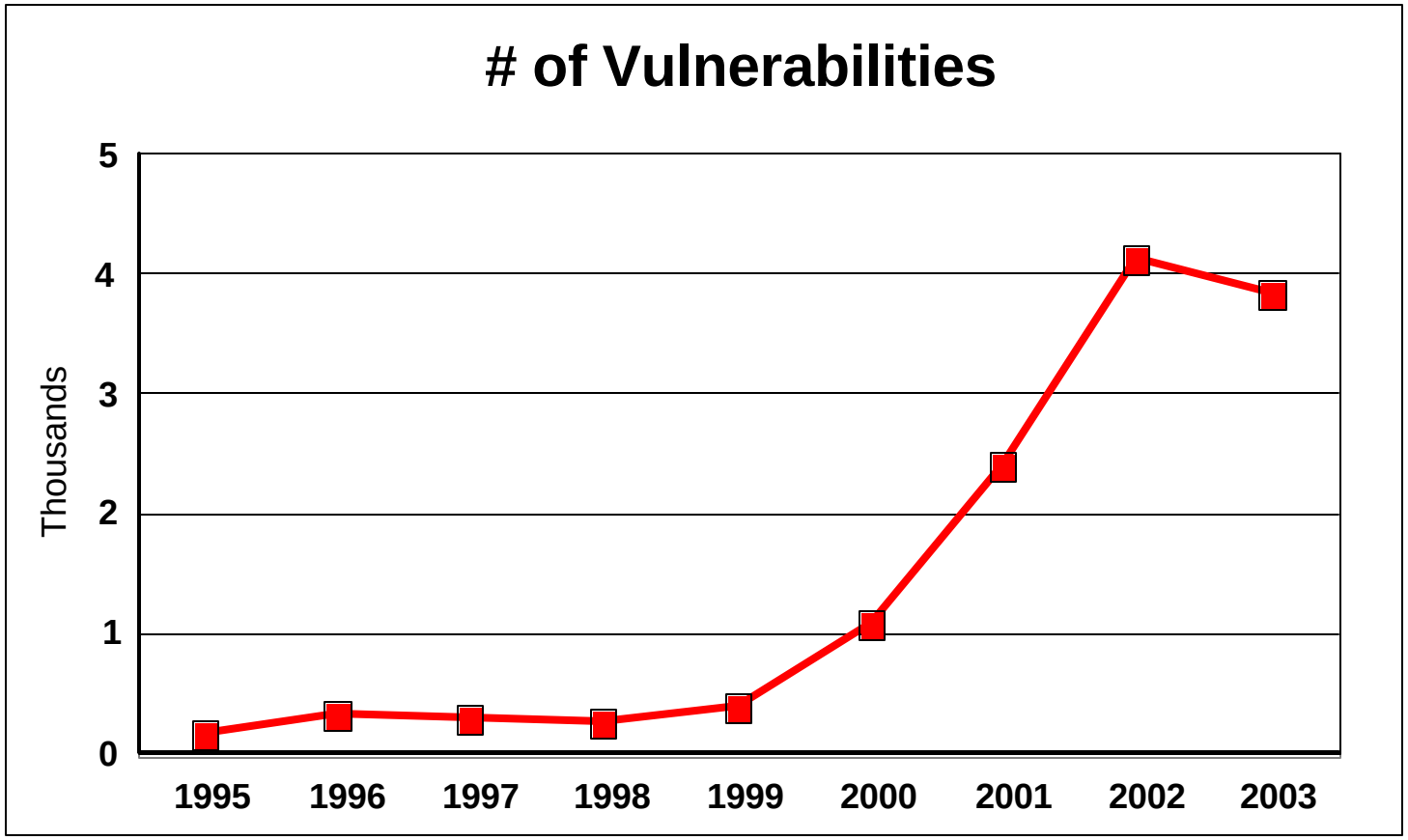


Number of Incidents



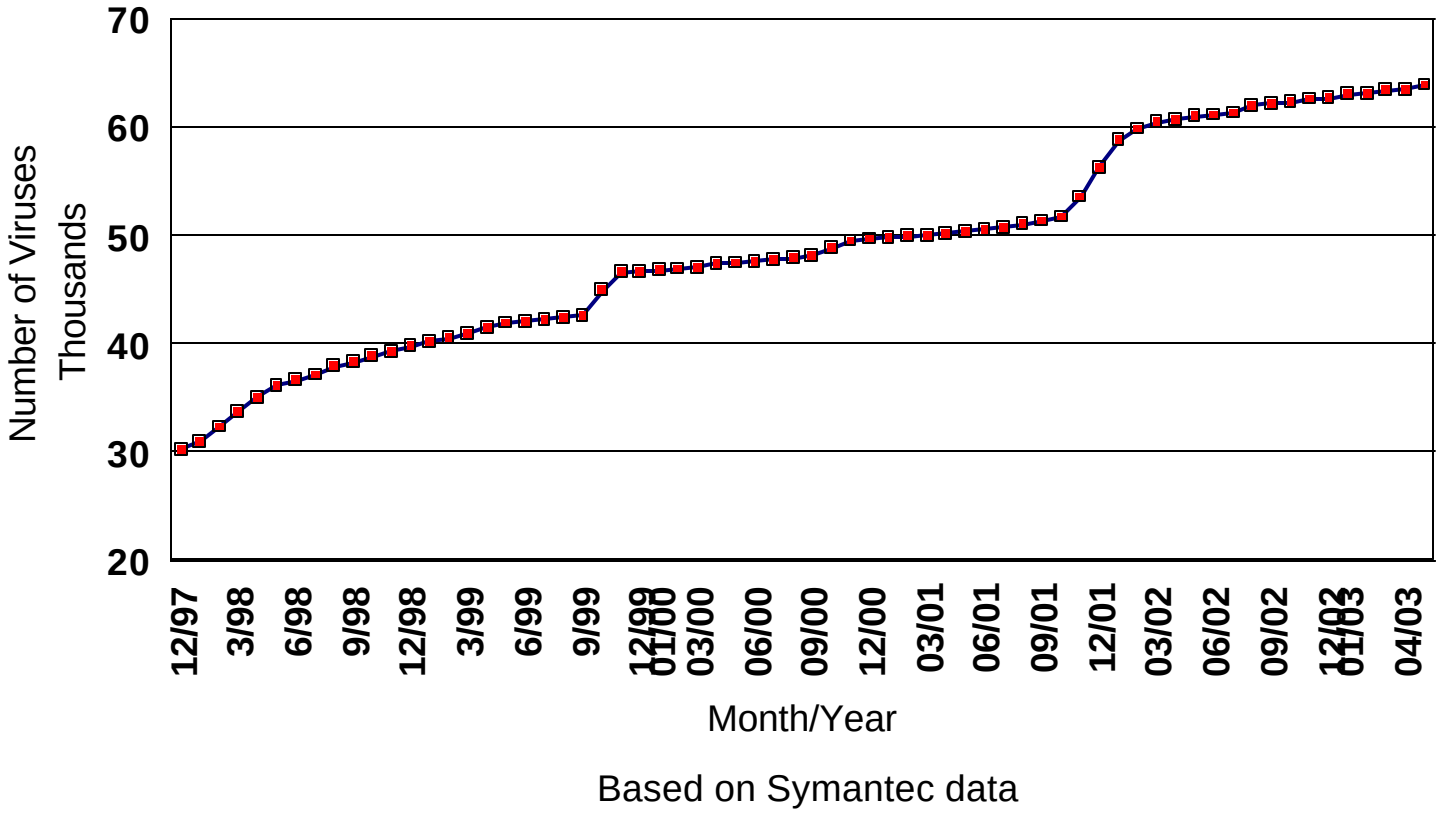
2003 Q1 = 42,586

Number of New Vulnerabilities



2003 Q1 = 959

Malicious Code Growth



Based on Symantec data

Misconceptions of Security

Experience shows that ...

- **...Users do not want to remove existing vuln.,**
  - ✓ javascript, shared files, E-mail attachments ...
- **...Vulnerabilities can not be removed,**
  - ✓ unsupported OS, TCP-IP, SNMP, etc.
- **...New systems also contain "old" vuln.,**
- **... Secure + Secure ≠ Secure**

Real systems must cope with the existence of vulnerabilities.

Defending Your Site

- **Evaluate your security posture**
  - ✓ Comprehensive policies in place and in use
  - ✓ Systems configured securely and checked
- **Detect security violations**
  - ✓ Identify attacks before they become serious
  - ✓ Around-the-clock vigilance required
- **Respond to security incidents**
  - ✓ Containment, eradication, recovery
  - ✓ Know what to do and how
  - ✓ Speed is of the essence

What is IDS

What is IDS?

- ✓ IDS protects e-business by continuously watching critical networks & systems for patterns of misuse or abuse. If systems are threatened, IDS can notify you or take precautionary actions to prevent information theft or loss.
- ✓ IDS compliments your Firewall by monitoring the following internal activities:
  - Network scans
  - DDoS Attacks
  - Excessive failed logins
  - Changes to system configuration & security settings
  - Changes to operating system, application or data files
  - Use of privileged accounts
  - Granting system privileges

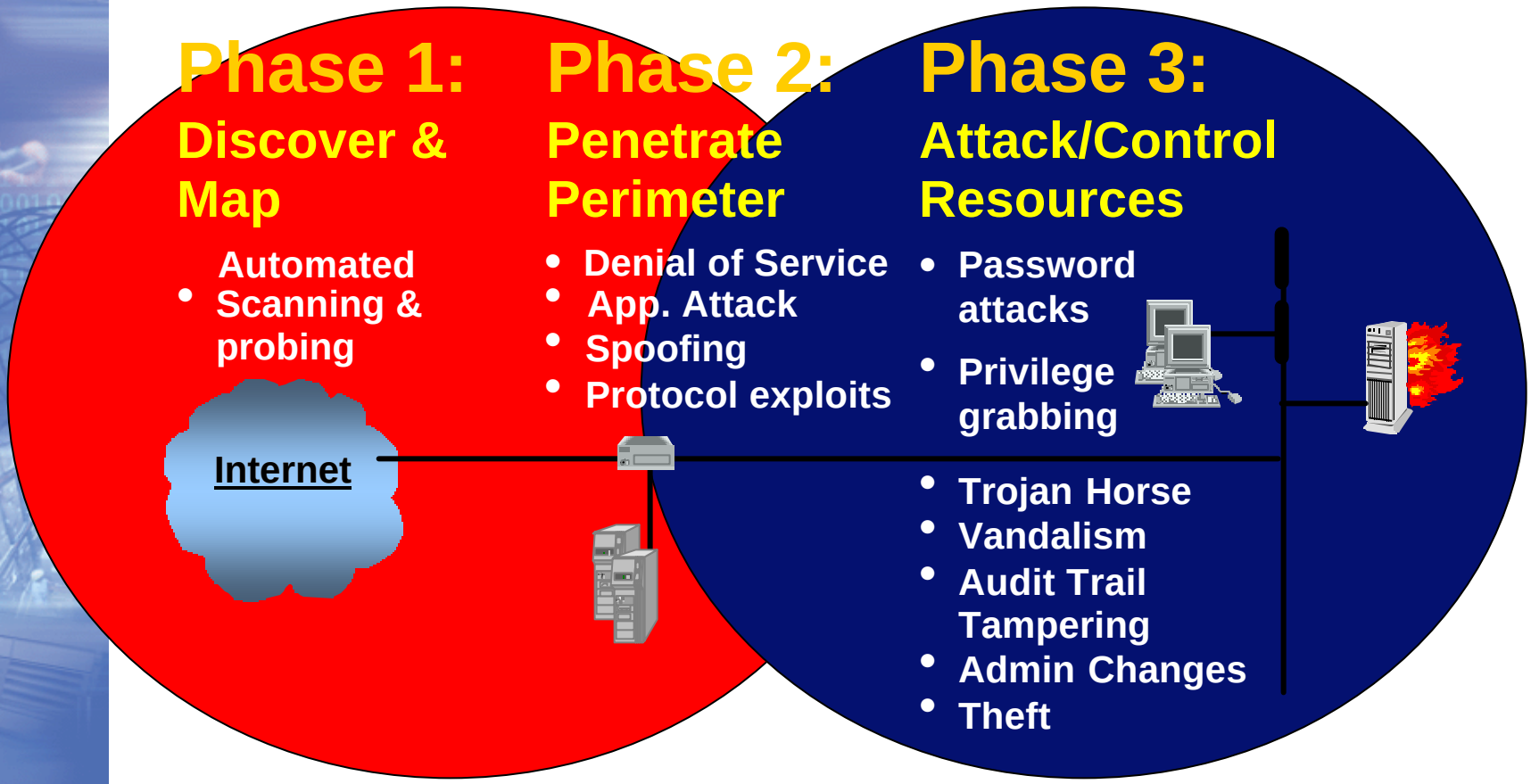
Why Deploy IDS?

- **Early Warning**
  - **“You Don’t Know What You Don’t Know.”**
  - **Detection of “pre attack” reconnaissance”**
  - **Nobody likes to be watched**
  - **Minimization of reaction and recovery time**
  - **Reduction of chances of success**
  - **Minimization of recovery time**
- **Threat Documentation**
  - **Quantification of the problem**
  - **Quantification of effectiveness of policy**
  - **Helps drive improvement in security posture**
  - **Helps support security funding/spending**
- **Helps Demonstrates Due-Diligence**
  - **Detection of outbound attacks**
  - **DDOS Liability**
  - **Answering to “Irving”**

Types of IDS

- Host Based IDS
  - Agents deployed on critical systems
  - Monitors system:
    - Processes
    - Configurations
    - File systems
    - Log files
    - Other system parameters
- Network IDS
  - Deployed at critical network junctions
    - Outside of DMZ
    - Inside of DMZ
    - Critical subnets
    - Extranet connections
  - Signature based
  - Future – Heuristic attack detection

Network and Host IDS Partnership



Common IDS Techniques

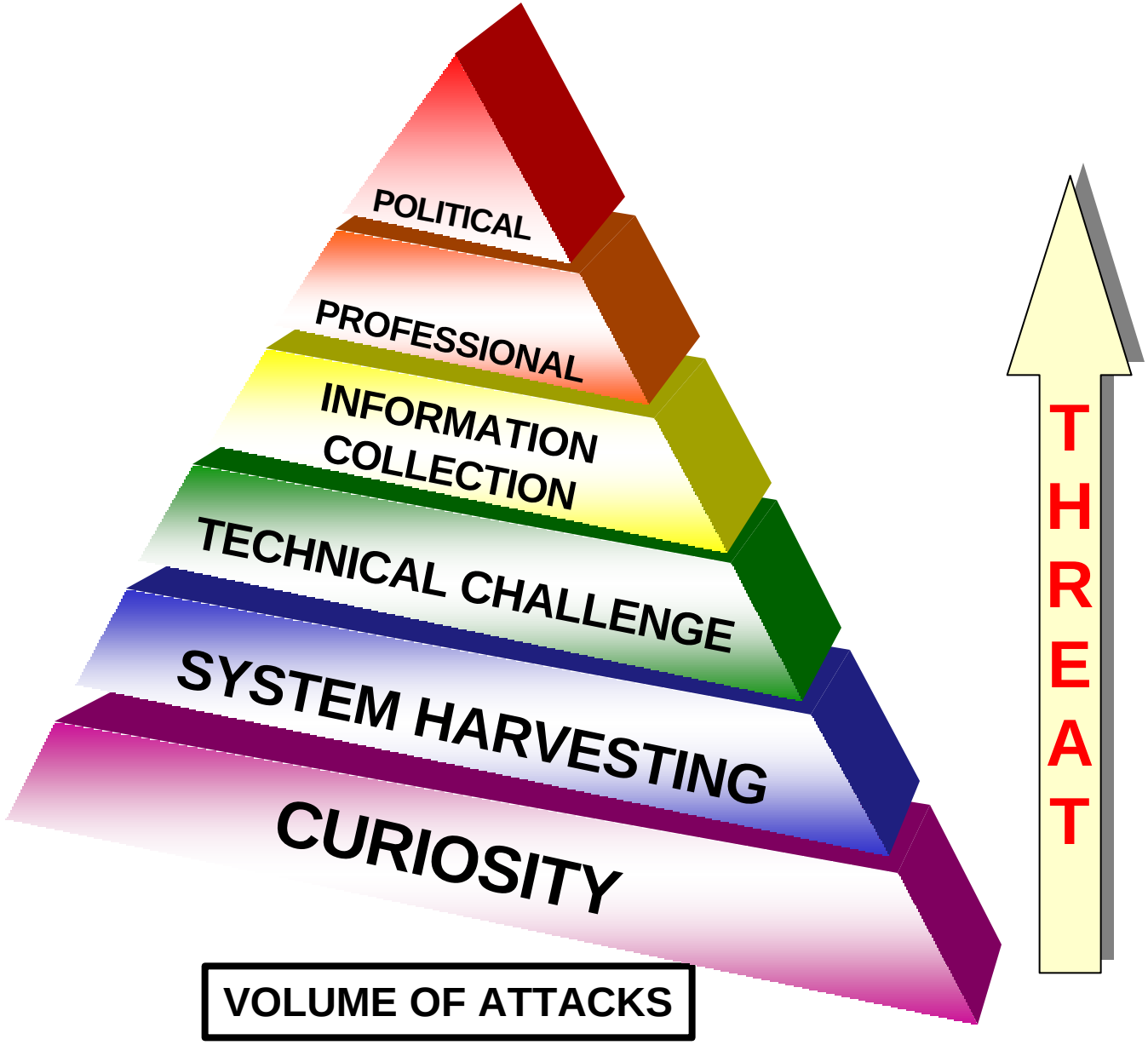
- **Statistical Analysis**
  - ✓ summary, profile, trend analysis
- **Expert System or Knowledge-based**
  - ✓ rules about known vulnerabilities, user profiles
- **Signature Analysis**
  - ✓ Identify specific behavior
    - subject: owner of the event
    - object: target of the event
    - action: what caused the event
    - context: condition of the event

Deploying an IDS Solution
Data to Knowledge

Overview of Types of Attacks

- Motive & Skill
- Reconnaissance
- Vulnerability mapping
- Initial access
- Privileged access
- Covert access

Hacker Motive & Skill



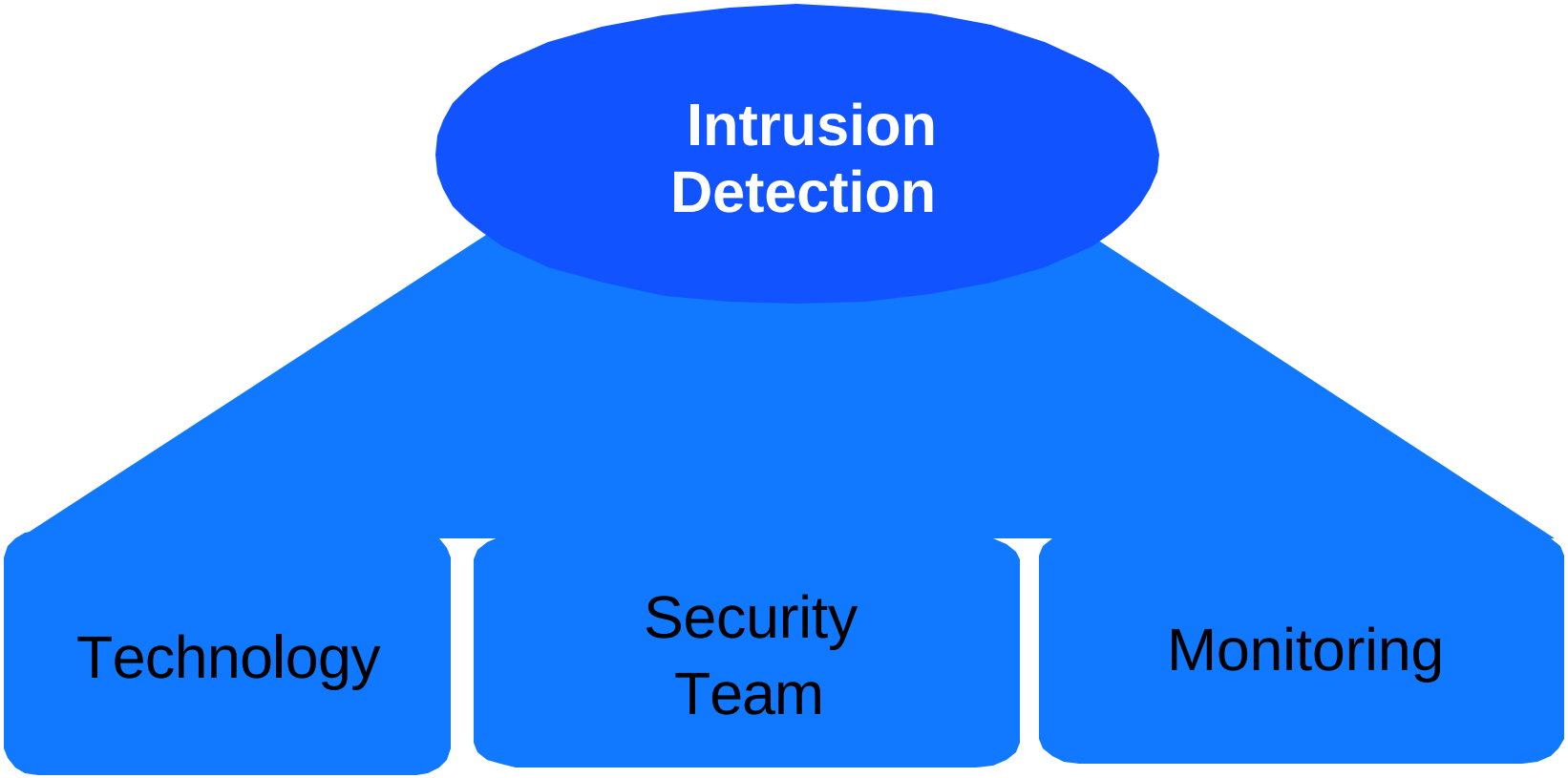
Target or Opportunity

- **Network is specifically targeted**
  - ✓ Corporate identity / ownership (ibm.com)
  - ✓ Associated with identity / cause

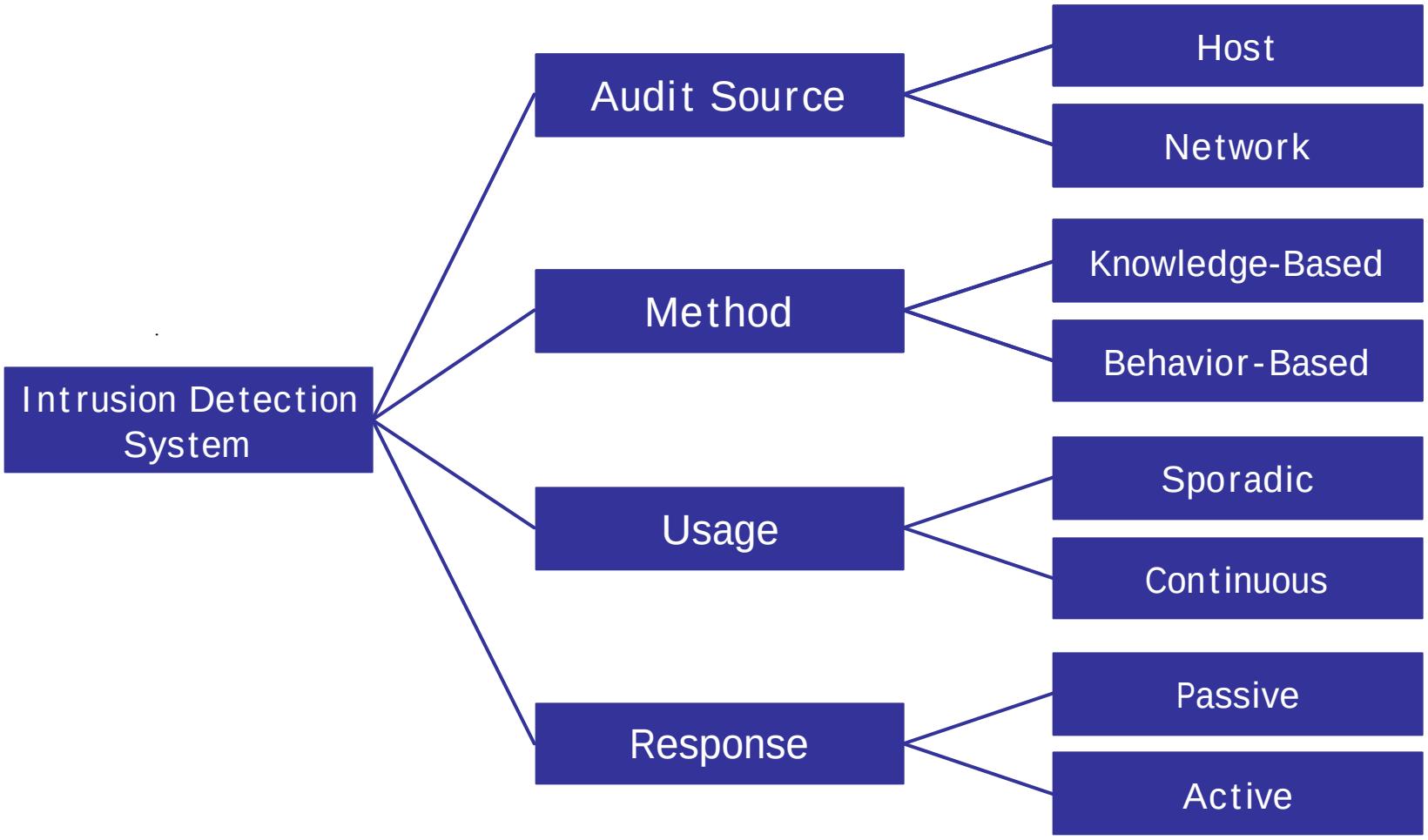
Or

- **Network is target of opportunity**
  - ✓ Identified by automated tools
  - ✓ Vulnerable
  - ✓ Purely random

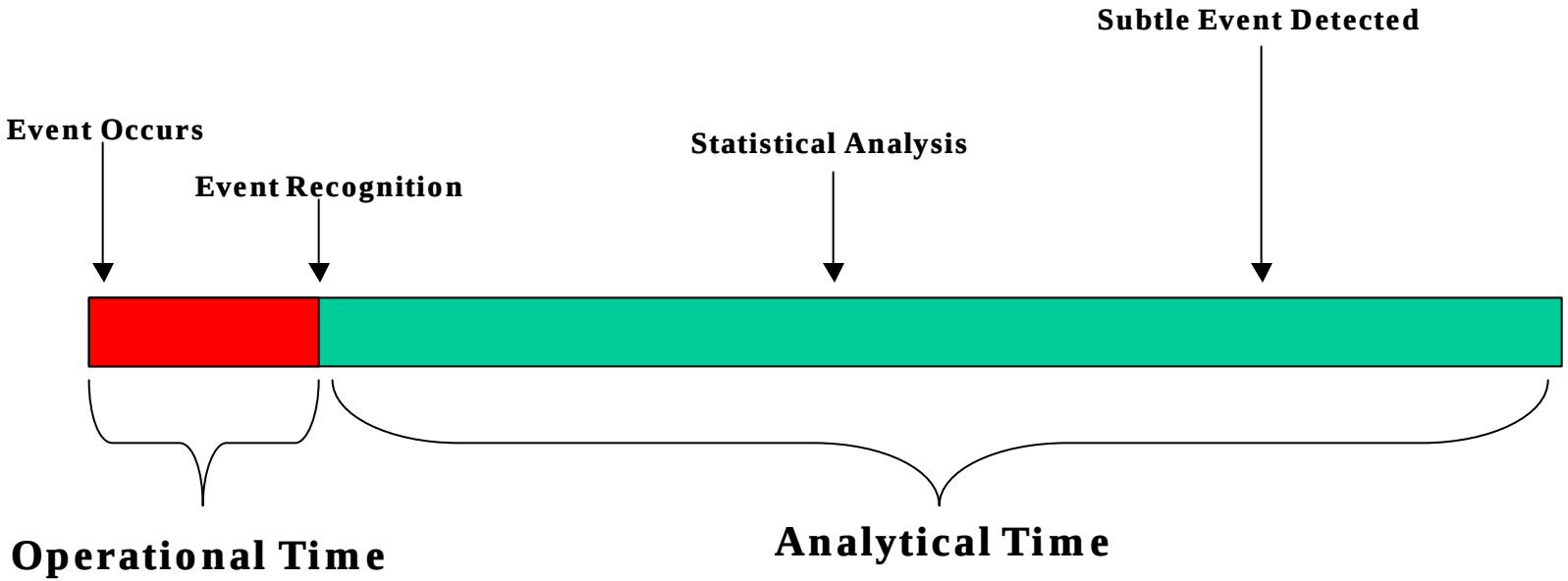
The Parts of an IDS Solution



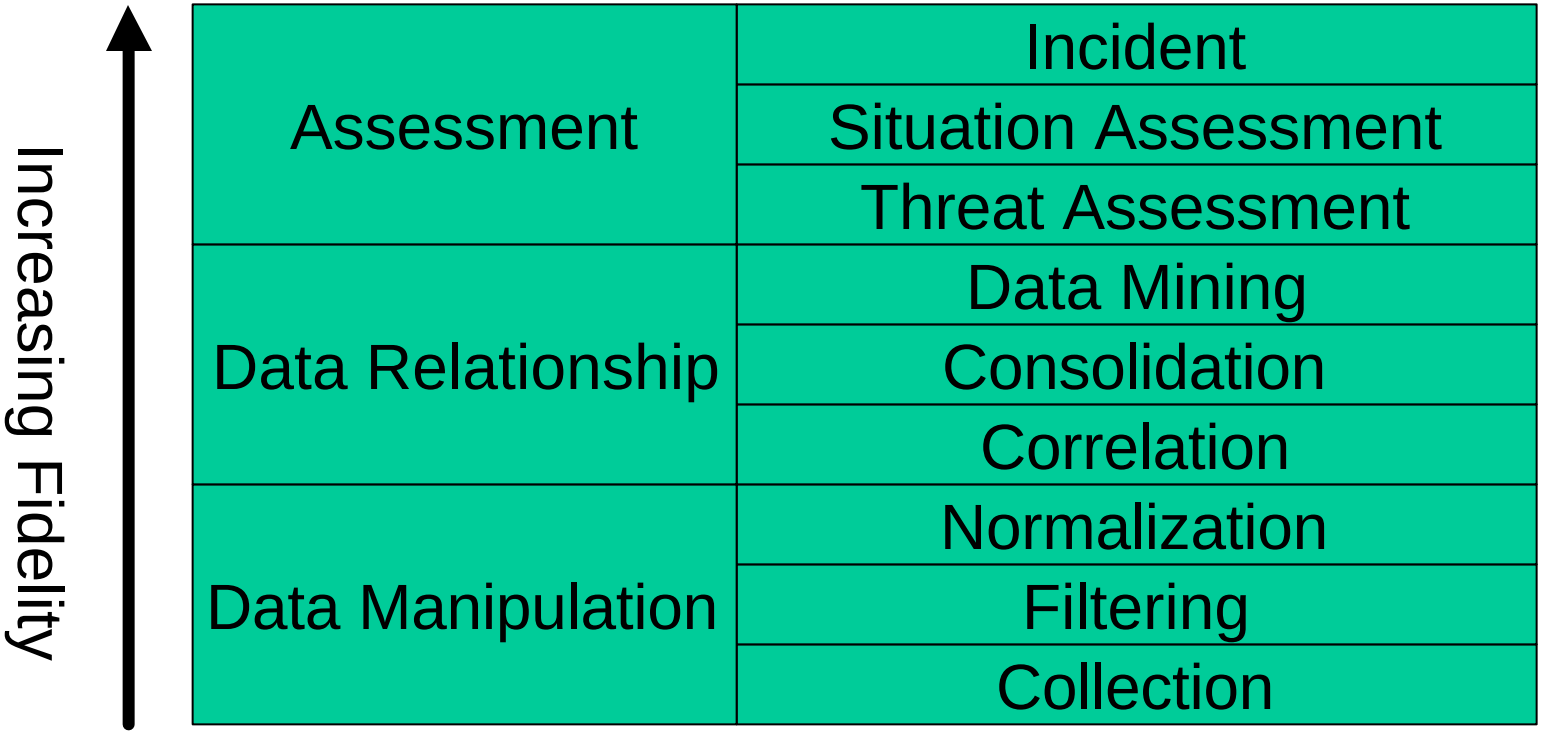
IDS Characteristics



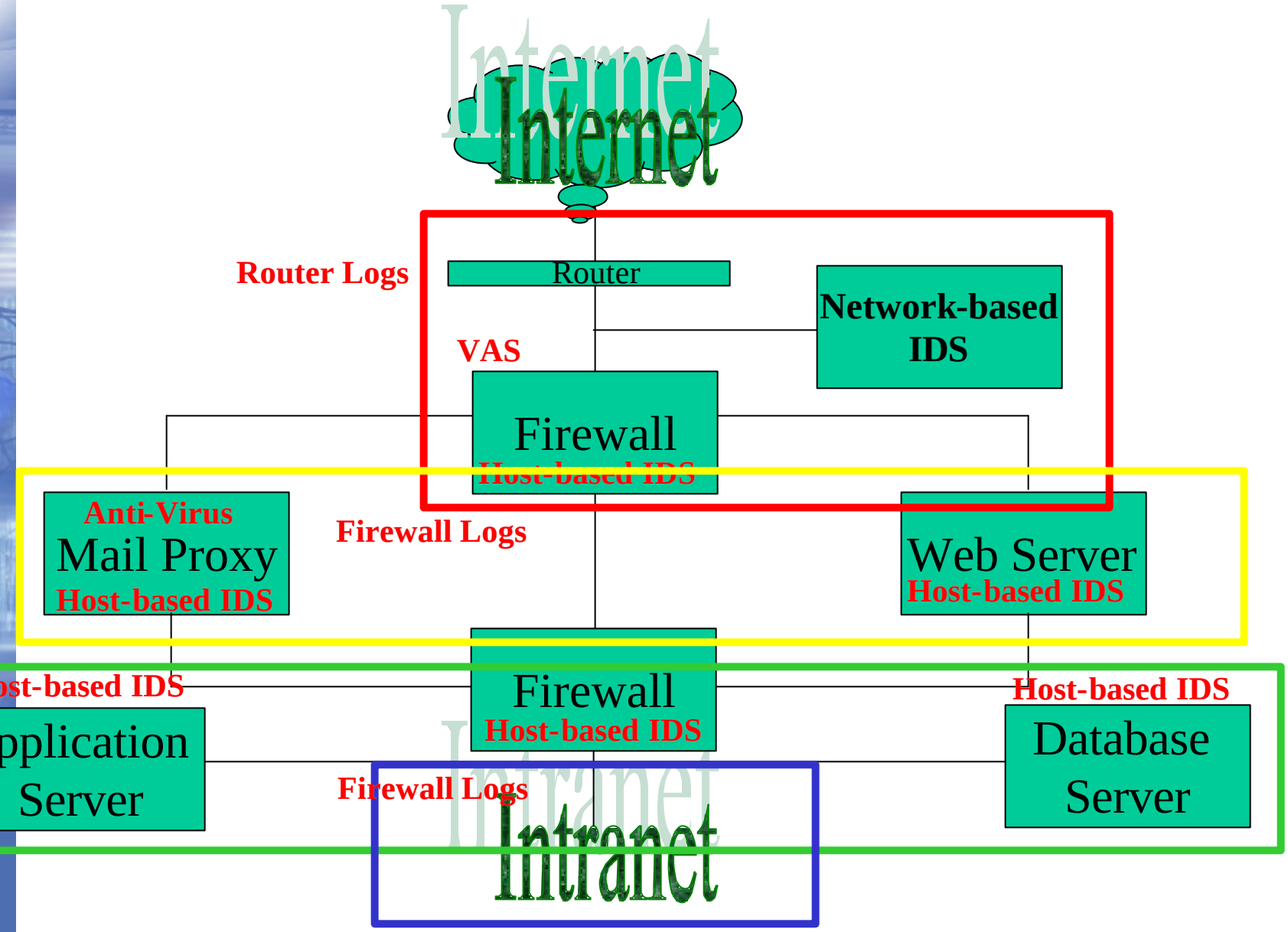
Monitor, Recognize & React



IDS Management



Collection


Internet
Router Logs
Router
Network-based IDS
VAS
Firewall
Host-based IDS
Anti-Virus
Mail Proxy
Host-based IDS
Firewall Logs
Web Server
Host-based IDS
Host-based IDS
Application Server
Firewall
Host-based IDS
Host-based IDS
Database Server
Firewall Logs
Intranet

What We Want to Avoid

Filtering & Anomaly Detection

- **Idea: Only look at what's new/anomalous**
- **Problem: Risk to discard true positives**
- **Solution: Use data mining to**
  - ✓ Understand alarms and their root causes
  - ✓ Preferably resolve root causes (fix, block, patch, ...)
  - ✓ Use well-understood filters when resolving is no option
- **Conclusion: The alarm load is reduced by a controlled and safe process**
  - ✓ Minimal risk of discarding true positives
  - ✓ Reduced alarm load improves service quality

Filtering
False Positives

- **Host-based IDS**
  - ✓ 0% - 90%
- **Network-based IDS**
  - ✓ Initially > 90%
  - ✓ Ideally < 5%

Network-based Alarms

- **Average sensor receives about 1M alerts per week**
  - ✓ Level 1 -- 82%
  - ✓ Level 2 -- 18.08%
  - ✓ Level 3 -- 0.04%

Normal Business or Hacked Every Day

Coverage:	7157 out of 7392 alarms!
Alarm:	SNMP Suspicious Get
SrcIP/SrcPort:	228.xxx.13.106 / [1025,4890]
DstIP/DstPort:	228.xxx.13.1 / 161
Context:	... Oid Matched =S '1.3.6.1.2.1.2.2' ...
Time Structure:	Periodic with period 5 min

Interpretation: Network management tool:

-- Periodicity
-- Same cluster in previous months
-- Source and destination belong to customer
-- Destination is a router, Oid is traffic counter
-- Unlike hacking behavior

Nimda

Coverage:	16493 out of 35808 alarms!
Alarm:	WWW WinNT cmd.exe Access
SrcIP/SrcPort:	228.xxx.*.* / [1099, 45815]
DstIP/DstPort:	228.xxx.13.* / 80
Context:	... ../winnt/system32/cmd.exe', QUERY ...
Time Structure:	bursty
Interpretation:	NIMDA -- Worm that preferably attacks adjacent network blocks -- Source network is not customer network

Normalization

- **What to normalize on?**
  - ✓ Time
  - ✓ Attack Profile
    - DDoS
    - Malicious Code
  - ✓ CVE
  - ✓ Source
  - ✓ Target

Normalization

- *Definition:* Identify candidate events belonging to the same categories and groups them into subgroups or "clusters"

- IDS Knowledge Base
  - Databases (callout logs, knowledge of your environment)
  - Industry Statistics (from MSSP)

- Signature Encyclopedia

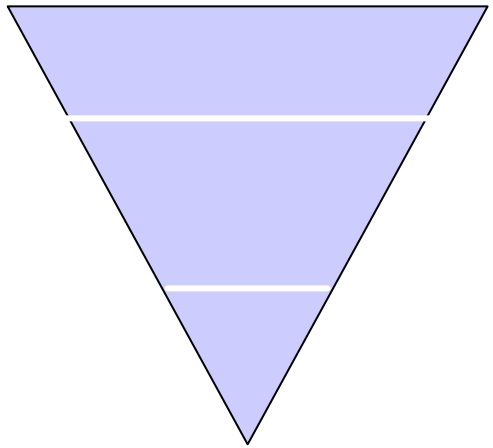
- Classification of Attack Types

Aggregation

- Definition: Displaying a single event with a count function to reduce analyst load in analyzing large event sequences.

- Sensor Level
- IDS Infrastructure
- IDS Console

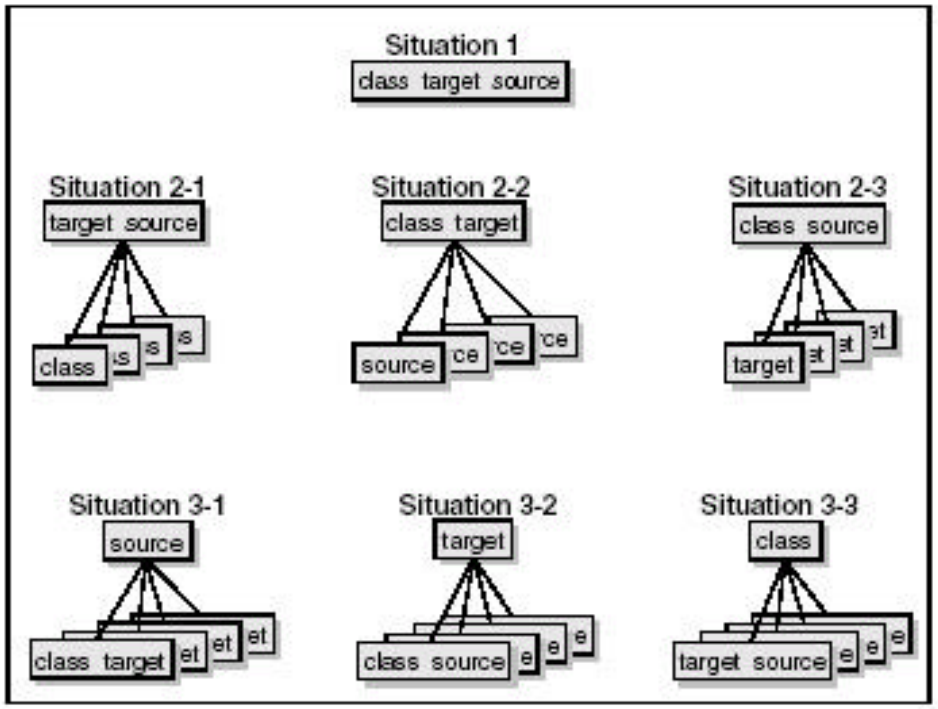
Compounding Aggregation



Correlation

Taking pieces of data from disparate data sources and combine them in meaningful ways to illustrate the situation or create a larger picture of the systems involved.

Examples of Correlation Rules



Example of Engine definition (correlation) in XML:

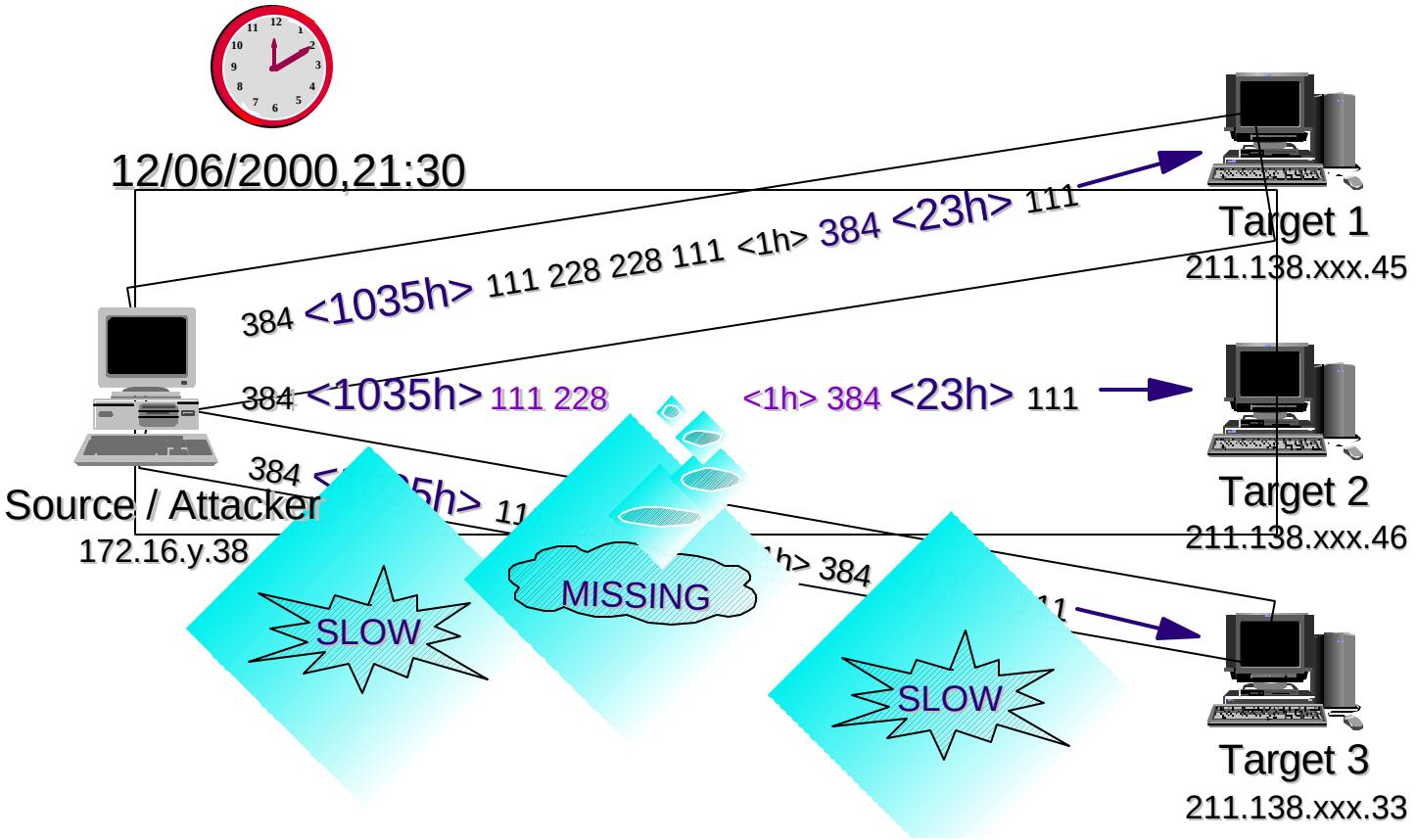
```
<engine name="correlation" class="com.tivoli.RiskManager.Agent.Engine.Engine" persist="NO">
<set key="RMA_conf" value="C:\RiskManager41\RISKMGR\etc\incident_engine.conf" />
</engine>
```

Consolidation

- **Correlation – Many events to one intrusion**
- **Consolidation – Many events to multiple intrusions**
- **Also know as Post-Event Correlation**

- **Low & slow attacks are**
  - ✓ Hard to detect because their trace is minimal
  - ✓ Dangerous because indicative of dedicated attackers
- **Detection of slow & low attacks**
  - ✓ Group/correlate alarms over prolonged timeframes
  - ✓ Reassess the combined severity, and
  - ✓ Raise meta-alerts when severity exceeds a threshold

Low and Slow attack



Cross-customer Consolidation

... in the month of October'01

Sources / Attackers		Target
202.128.131.172, 209.196.44.88, 217.35.104.29, ...	**1 Probe**	MSS Customer X

- Cross-sensor correlation caught these very low attacks
  - 202.128.131.172 — **45 Probes** — 31 MSS customers
  - 209.196.44.88 — **54 Probes** — 21 MSS customers
  - 217.35.104.29 — **25 Probes** — 22 MSS customers

By the way!

- **These attackers were not only very low, but also extremely slow!**
  - ✓ 202.128.131.172 : 45 probes over 17 days!
  - ✓ 209.196.44.88 : 54 probes over 10 days!
  - ✓ 217.35.104.29 : 25 probes over 5 days!
- **Conclusion: Cross-sensor correlation is a reliable way to detect the lowest and slowest attacks!**

Data Mining

- **Pattern Matching**

- **Many techniques and sub-techniques**
- **Clustering, classification, association rules, regression, ...**
- **Key question: Which one is most appropriate?**
  - ✓ Each technique has drawbacks of its own
  - ✓ Results that are trivial, hard to understand, redundant, misleading, ..

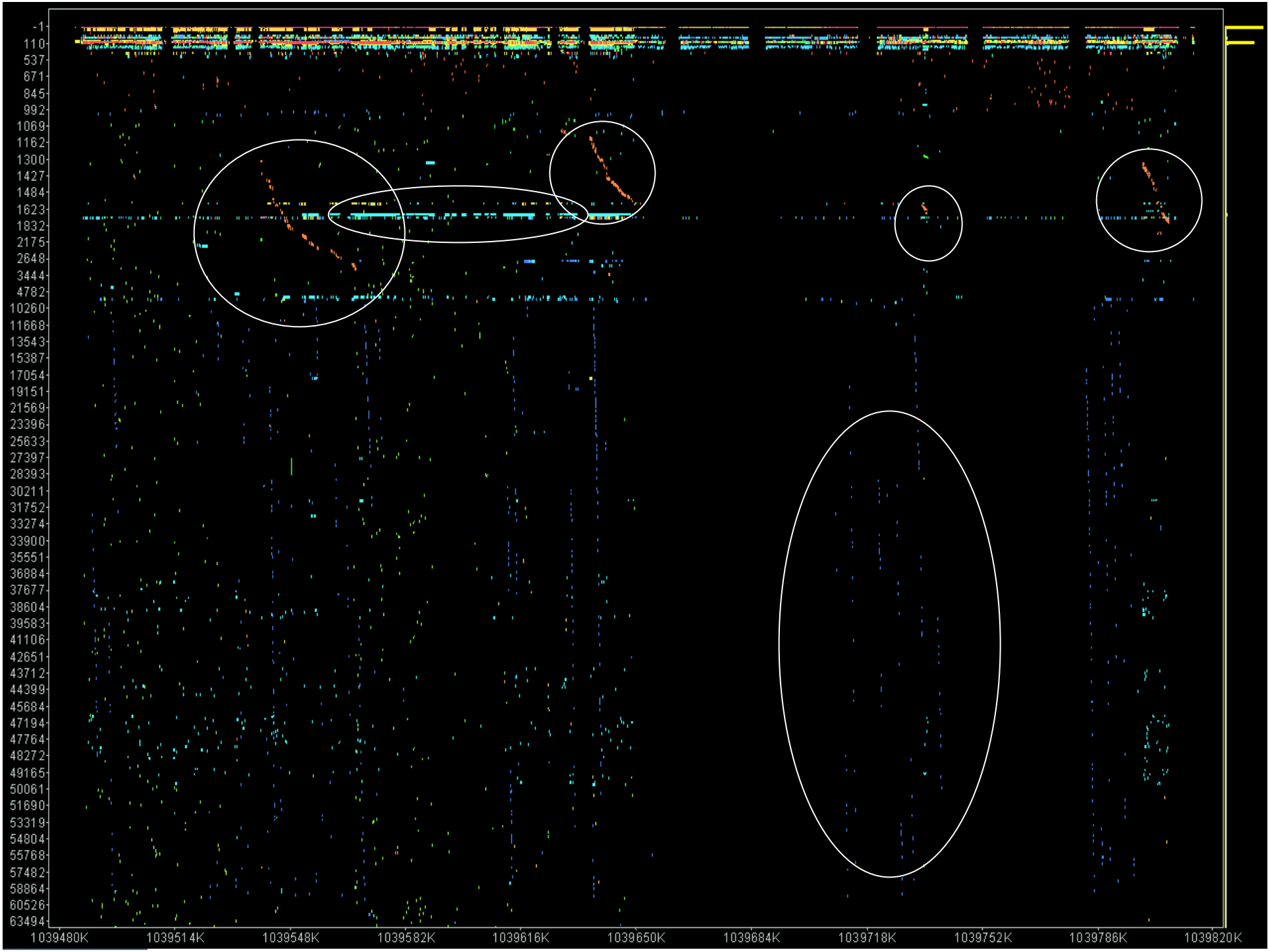
Assessment
Effectiveness of Alarms

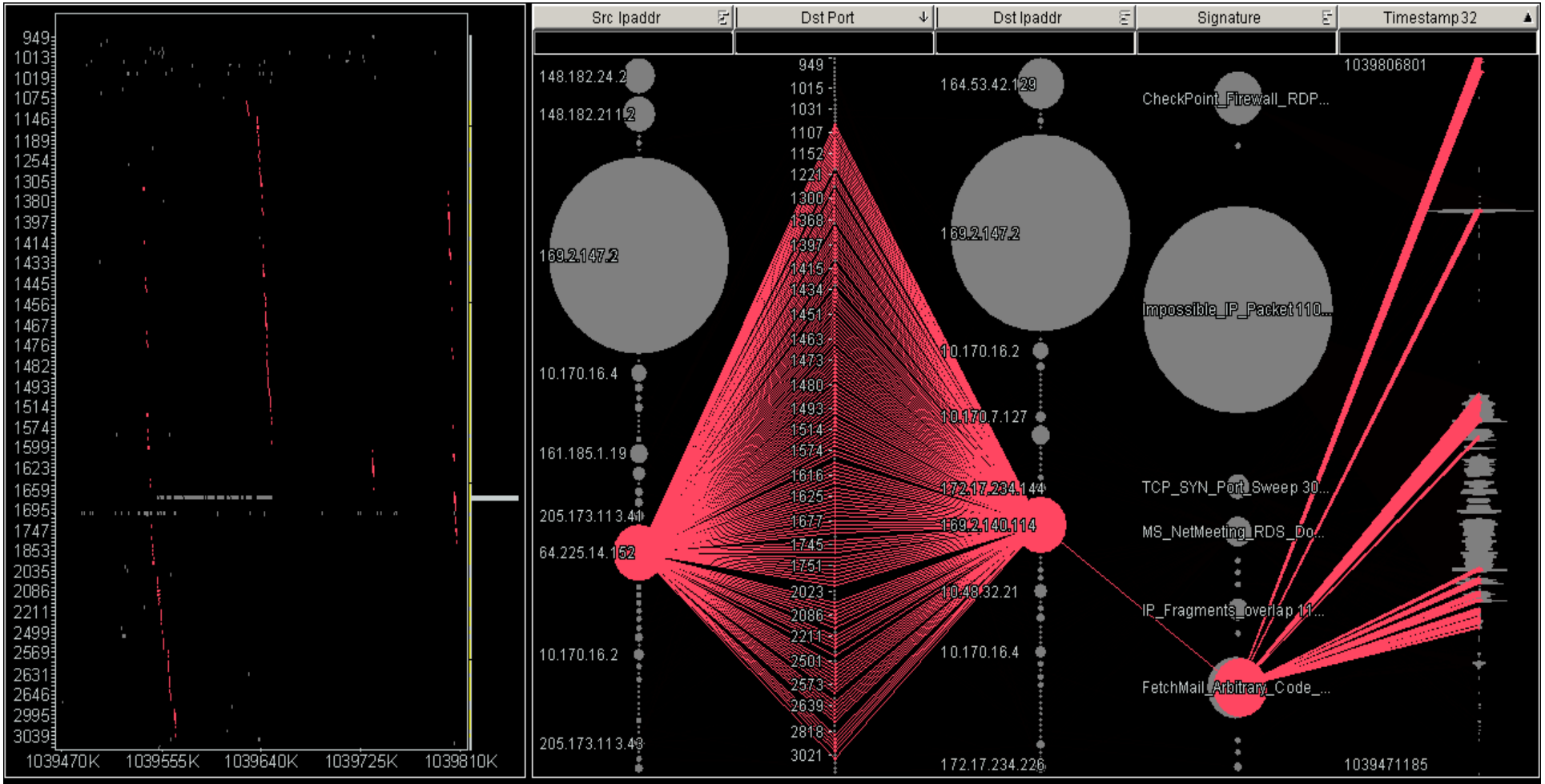
- **Threat Assessment**
  - ✓ Understanding whether or not the system is susceptible
- **Situation Assessment**
  - ✓ Understanding how critical the system is
- **Incident**
  - ✓ Knowing when and how long a system has been under attack

Assessment Examples

- **Unix based web servers**
  - ✓ IIS buffer overflow signatures
  - ✓ High alarm level.
- **Why not filter them out?**
  - ✓ We like to keep a eye on the network
  - ✓ Keeping vulnerabilities a customer isn't susceptible to helps with the big picture

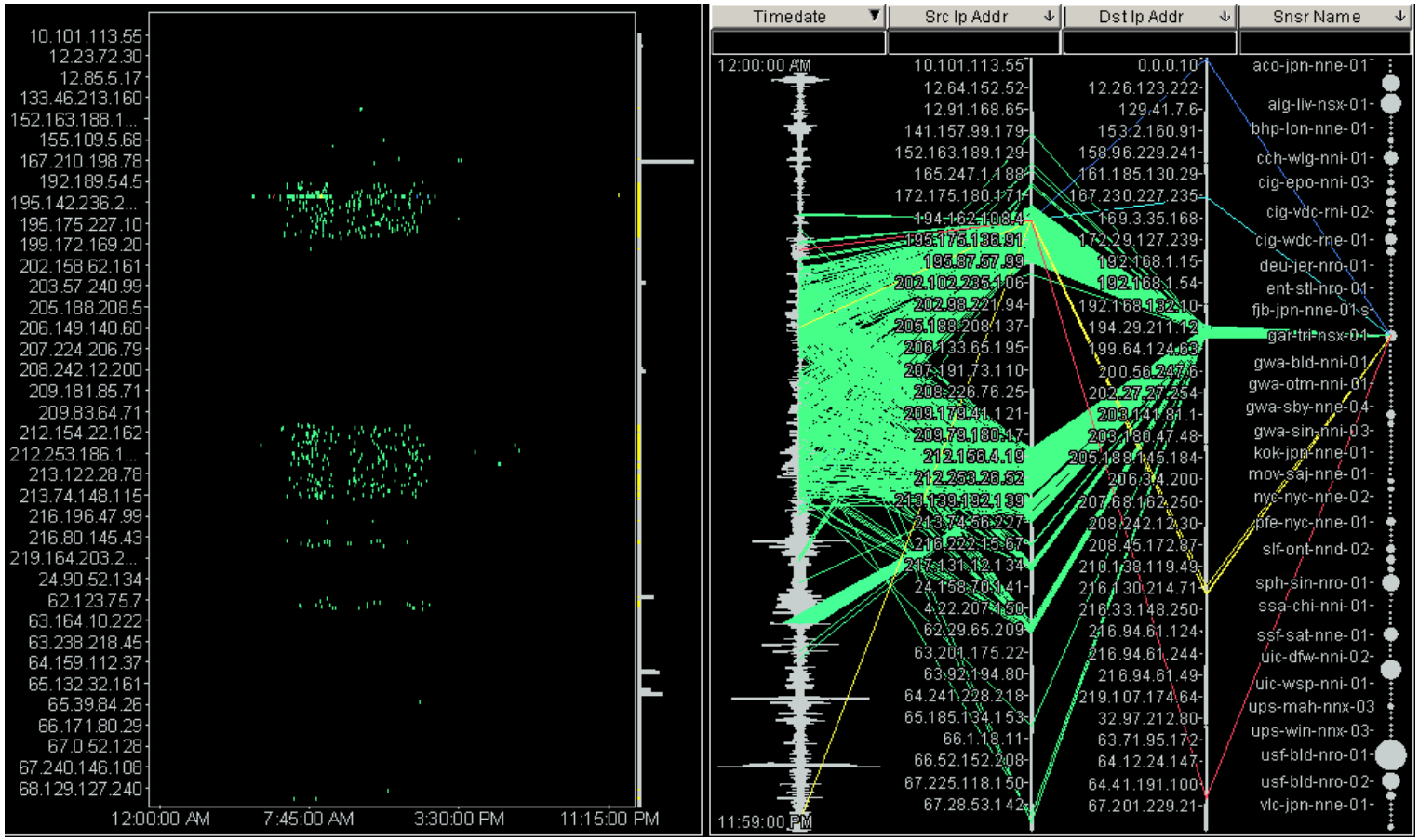
Using Data Visualizing Tools


-1
110
537
671
845
992
1069
1162
1300
1427
1484
1623
1832
2175
2648
3444
4782
10260
11668
13543
15387
17054
19151
21569
23396
25633
27397
28393
30211
31752
33274
33900
35551
36884
37677
38604
39583
41106
42651
43712
44399
45684
47194
47764
48272
49165
50061
51690
53319
54804
55768
57482
58864
60526
63494
1039480K
1039514K
1039548K
1039582K
1039616K
1039650K
1039684K
1039718K
1039752K
1039786K
1039820K



Src Ipaddr	Dst Ipaddr	Dst Port	Severity	Signature	Timestamp32
64.225.14.152	169.2.140.114	1326	4	FetchMail_Arbitrary_Code_Execution 3114 0	1039539805
64.225.14.152	169.2.140.114	1599	4	FetchMail_Arbitrary_Code_Execution 3114 0	1039544185
64.225.14.152	169.2.140.114	1968	4	FetchMail_Arbitrary_Code_Execution 3114 0	1039548569
64.225.14.152	169.2.140.114	2305	4	FetchMail_Arbitrary_Code_Execution 3114 0	1039554280
64.225.14.152	169.2.140.114	2646	4	FetchMail_Arbitrary_Code_Execution 3114 0	1039562755
64.225.14.152	169.2.140.114	1469	4	FetchMail_Arbitrary_Code_Execution 3114 0	1039644629
64.225.14.152	169.2.140.114	1305	4	FetchMail_Arbitrary_Code_Execution 3114 0	1039639910
64.225.14.152	169.2.140.114	1307	4	FetchMail_Arbitrary_Code_Execution 3114 0	1039640096
64.225.14.152	169.2.140.114	1625	4	FetchMail_Arbitrary_Code_Execution 3114 0	1039735557
64.225.14.152	169.2.140.114	1625	4	FetchMail_Arbitrary_Code_Execution 3114 0	1039735149
64.225.14.152	169.2.140.114	1473	4	FetchMail_Arbitrary_Code_Execution 3114 0	1039644587
64.225.14.152	169.2.140.114	1473	4	FetchMail_Arbitrary_Code_Execution 3114 0	1039644995
64.225.14.152	169.2.140.114	1476	4	FetchMail_Arbitrary_Code_Execution 3114 0	1039644770

Post Event Correlation



Real World Example

Excerpt from Daily Report

February 1, 2003 (Saturday)

HTTP IIS DOT DOT EXECUTE Bug	Med	WWW	12	aa.bbb.cc.234	unknown	eee.ff.g.7	02/01 21:40
HTTP IIS DOT DOT DENIAL Bug	Med	WWW	10	aa.bbb.cc.234	unknown	eee.ff.g.7	02/01 21:40
WWW WinNT cmd.exe Access	High	WWW	14	aa.bbb.cc.234	unknown	eee.ff.g.7	02/01 21:40
WWW IIS Unicode Attack	High	WWW	2	aa.bbb.cc.234	unknown	eee.ff.g.7	02/01 21:40
WWW IIS Unicode Attack	High	WWW	1	aa.bbb.cc.234	unknown	eee.ff.g.7	02/01 21:40
WWW IIS Unicode Attack	High	WWW	1	aa.bbb.cc.234	unknown	eee.ff.g.7	02/01 21:40
WWW IIS Double Decode Error	Med	WWW	1	aa.bbb.cc.234	unknown	eee.ff.g.7	02/01 21:40
WWW IIS Double Decode Error	Med	WWW	4	aa.bbb.cc.234	unknown	eee.ff.g.7	02/01 21:40

TTP IIS DOT DOT EXECUTE Bug	Med	WWW	12	aa.bbb.cc.234	unknown	eee.ff.g..71	02/01 21:44
HTTP IIS DOT DOT DENIAL Bug	Med	WWW	10	aa.bbb.cc.234	unknown	eee.ff.g..71	02/01 21:44
WWW WinNT cmd.exe Access	High	WWW	14	aa.bbb.cc.234	unknown	eee.ff.g..71	02/01 21:44
WWW IIS Unicode Attack	High	WWW	2	aa.bbb.cc.234	unknown	eee.ff.g..71	02/01 21:44
WWW IIS Unicode Attack	High	WWW	1	aa.bbb.cc.234	unknown	eee.ff.g..71	02/01 21:44
WWW IIS Unicode Attack	High	WWW	1	aa.bbb.cc.234	unknown	eee.ff.g..71	02/01 21:44
WWW IIS Double Decode Error	Med	WWW	1	aa.bbb.cc.234	unknown	eee.ff.g..71	02/01 21:44
WWW IIS Double Decode Error	Med	WWW	4	aa.bbb.cc.234	unknown	eee.ff.g..71	02/01 21:44
Root.exe access	High	WWW	2	aa.bbb.cc.234	unknown	eee.ff.g..71	02/01 21:44

Excerpt from Daily Report

- **February 1, 2003 (Saturday)**

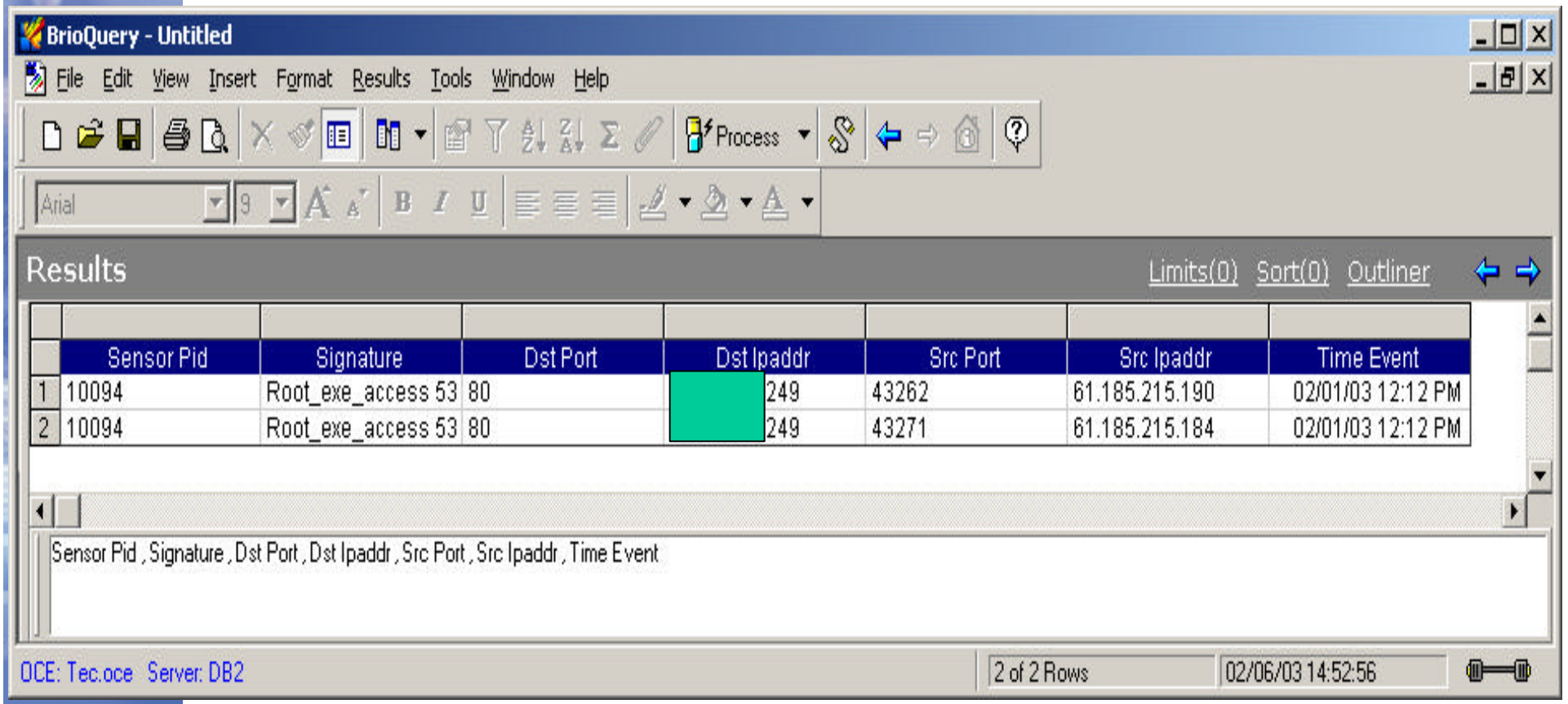
Net Sweep-Echo	Low Recon	1	61.177.115.188	unknown	0.0.0.0	02/01 08:00
Net Sweep-Echo	Low Recon	1	61.177.115.188	unknown	aa.bb.ccc.249	02/01 07:27
Net Sweep-Echo	Low Recon	1	61.177.115.188	unknown	aa.bb.ccc.9	02/01 08:00
Root.exe access	High WWW	1	61.185.215.184	unknown	aa.bb.ccc.249	02/01 18:12
Root.exe access	High WWW	1	61.185.215.190	unknown	aa.bb.ccc.249	02/01 18:12
Suspicious Mail Attachment	Low UnAcc	1	62.114.33.104	unknown	aa.bb.ccc.11	02/01 12:05

Root.exe access

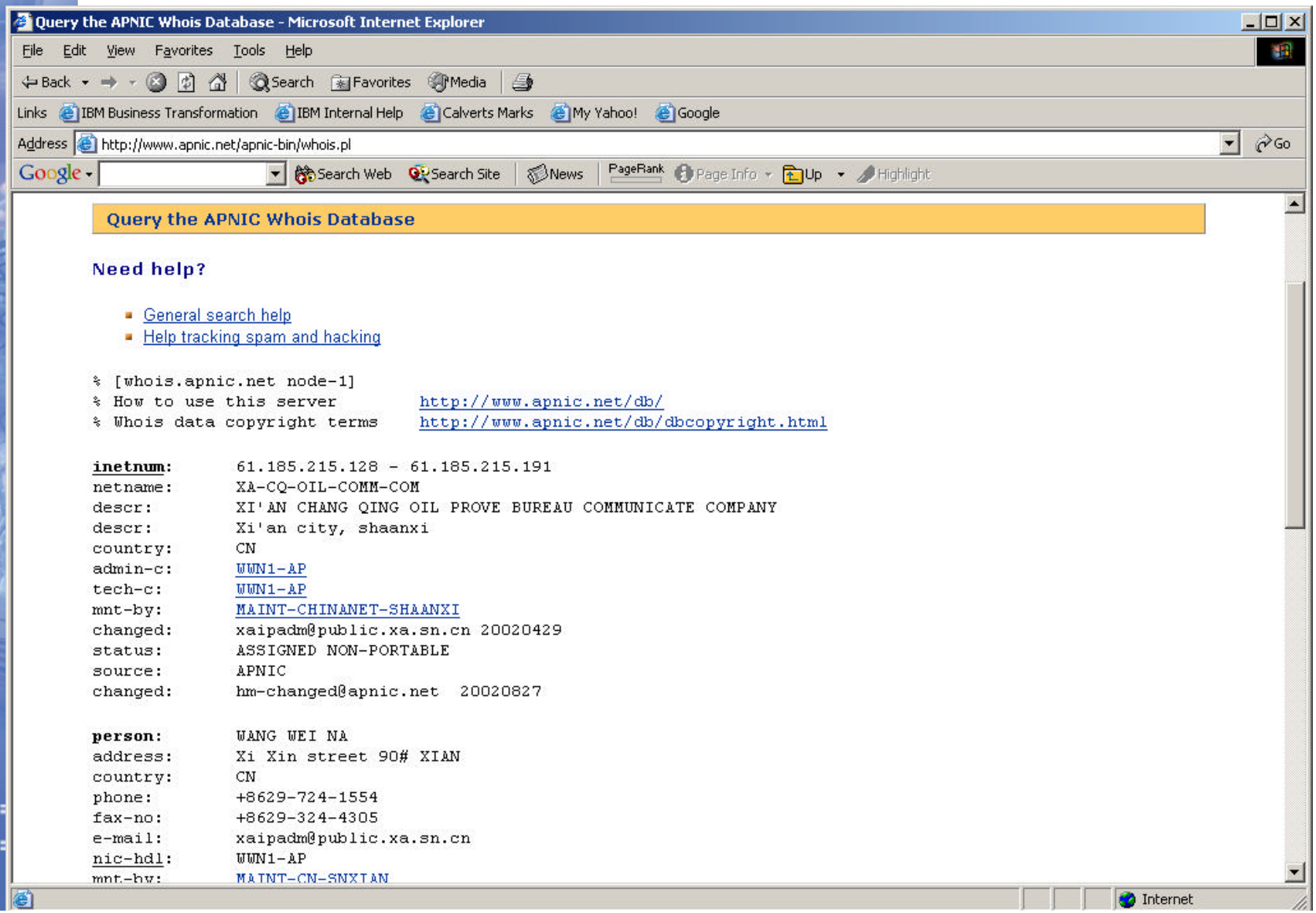
- This event triggers upon detecting a http request for root.exe. The NIMDA worm exploits vulnerabilities in Microsoft Internet Information Server (IIS), Internet Explorer (IE), and Outlook (MAPI) to infect workstations running Windows 95/98/ME, workstations running Windows NT/2000, and servers/domain controllers running Window NT/2000.

Countermeasure(s): It is highly recommended that organizations patch all Windows NT/2000 hosts running IIS (version 4.0 and 5.0) to mitigate IIS buffer overflows and Code Red II backdoors.

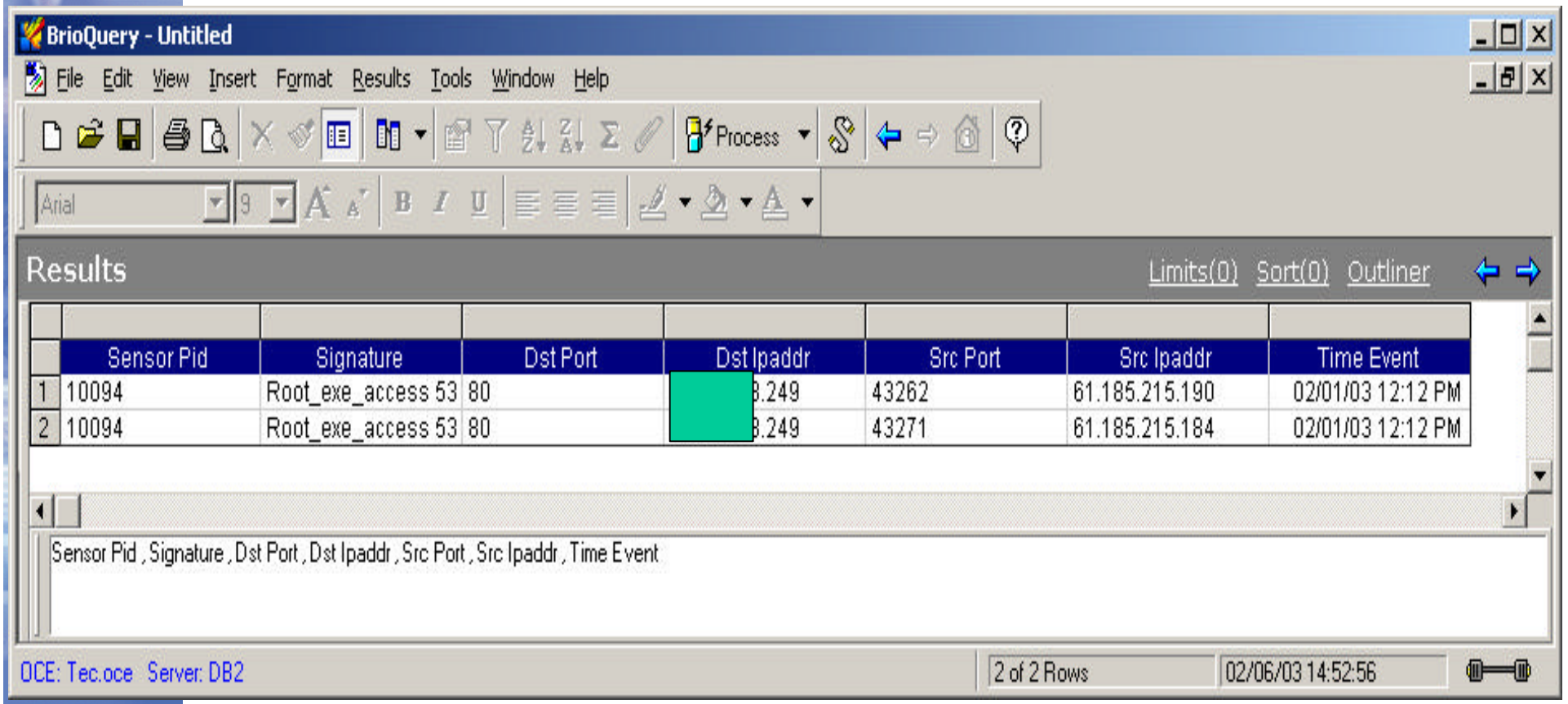
Brio Query of Suspicious Offenders Across the Customer's Network (.184,.190)



APNIC Lookup on Suspicious IP's

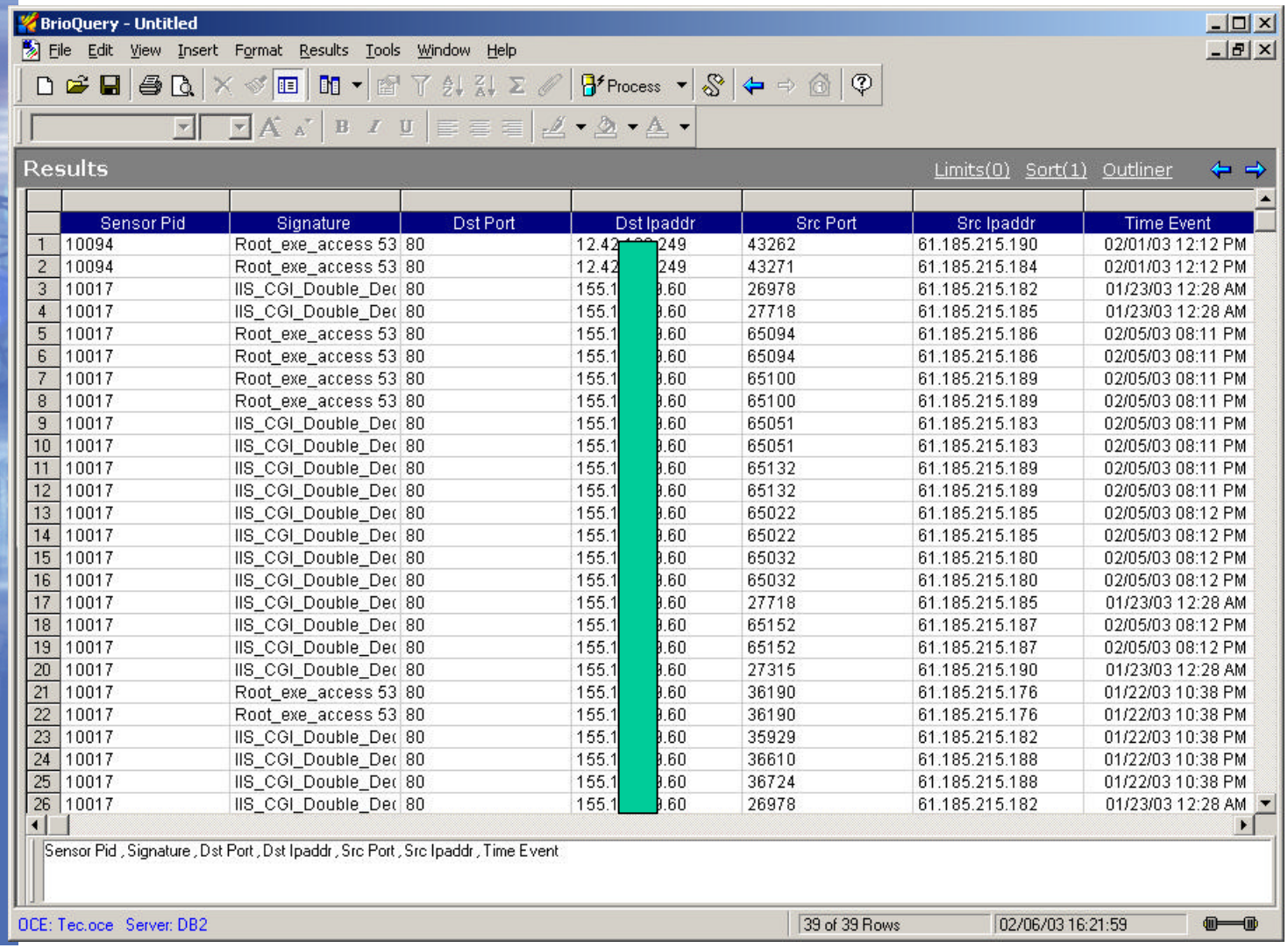


Brio Query of Suspicious Offenders (Partial Class C - 61.185.215.128-191) Across the Customer's Network

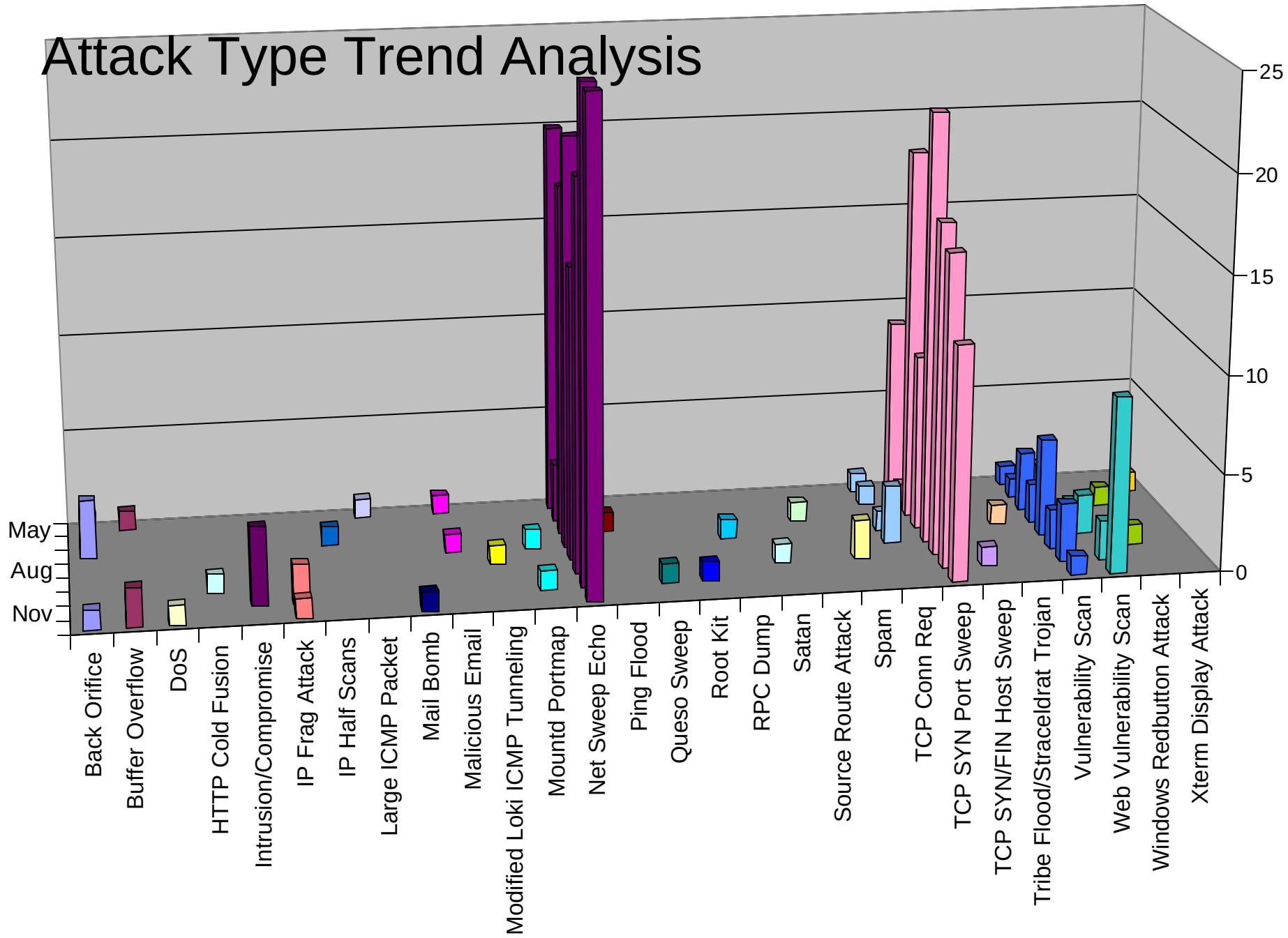


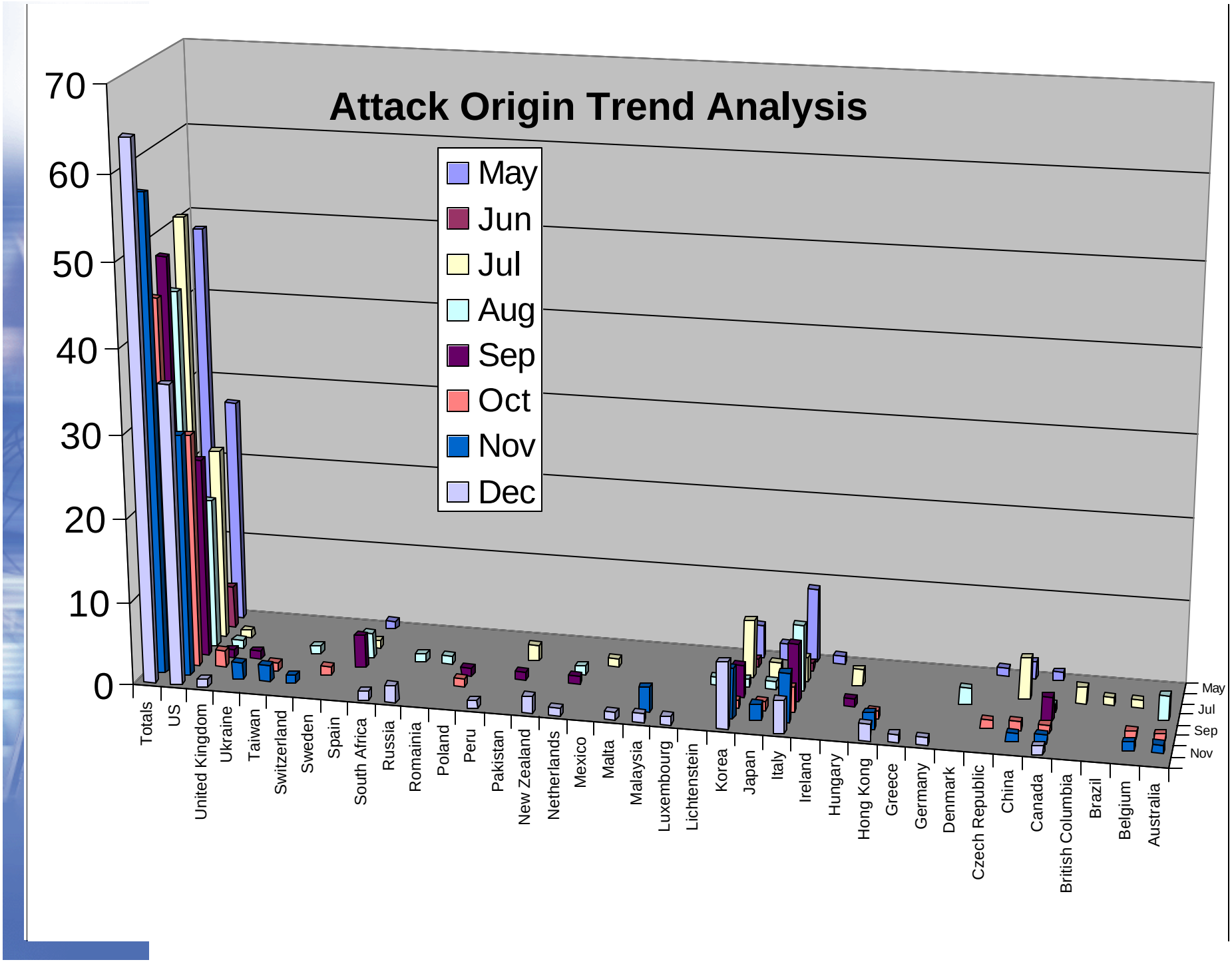
…same results. Only 2 attacks from Chinese oil company directed at RCL.

Brio Query of Suspicious Offenders (Partial Class C - 61.185.215.128-191) Across the Full Customer Set



	Sensor Pid	Signature	Dst Port	Dst Ipaddr	Src Port	Src Ipaddr	Time Event
1	10094	Root_exe_access 53	80	12.42 .249	43262	61.185.215.190	02/01/03 12:12 PM
2	10094	Root_exe_access 53	80	12.42 .249	43271	61.185.215.184	02/01/03 12:12 PM
3	10017	IIS_CGI_Double_Dec	80	155.1 .60	26978	61.185.215.182	01/23/03 12:28 AM
4	10017	IIS_CGI_Double_Dec	80	155.1 .60	27718	61.185.215.185	01/23/03 12:28 AM
5	10017	Root_exe_access 53	80	155.1 .60	65094	61.185.215.186	02/05/03 08:11 PM
6	10017	Root_exe_access 53	80	155.1 .60	65094	61.185.215.186	02/05/03 08:11 PM
7	10017	Root_exe_access 53	80	155.1 .60	65100	61.185.215.189	02/05/03 08:11 PM
8	10017	Root_exe_access 53	80	155.1 .60	65100	61.185.215.189	02/05/03 08:11 PM
9	10017	IIS_CGI_Double_Dec	80	155.1 .60	65051	61.185.215.183	02/05/03 08:11 PM
10	10017	IIS_CGI_Double_Dec	80	155.1 .60	65051	61.185.215.183	02/05/03 08:11 PM
11	10017	IIS_CGI_Double_Dec	80	155.1 .60	65132	61.185.215.189	02/05/03 08:11 PM
12	10017	IIS_CGI_Double_Dec	80	155.1 .60	65132	61.185.215.189	02/05/03 08:11 PM
13	10017	IIS_CGI_Double_Dec	80	155.1 .60	65022	61.185.215.185	02/05/03 08:12 PM
14	10017	IIS_CGI_Double_Dec	80	155.1 .60	65022	61.185.215.185	02/05/03 08:12 PM
15	10017	IIS_CGI_Double_Dec	80	155.1 .60	65032	61.185.215.180	02/05/03 08:12 PM
16	10017	IIS_CGI_Double_Dec	80	155.1 .60	65032	61.185.215.180	02/05/03 08:12 PM
17	10017	IIS_CGI_Double_Dec	80	155.1 .60	27718	61.185.215.185	01/23/03 12:28 AM
18	10017	IIS_CGI_Double_Dec	80	155.1 .60	65152	61.185.215.187	02/05/03 08:12 PM
19	10017	IIS_CGI_Double_Dec	80	155.1 .60	65152	61.185.215.187	02/05/03 08:12 PM
20	10017	IIS_CGI_Double_Dec	80	155.1 .60	27315	61.185.215.190	01/23/03 12:28 AM
21	10017	Root_exe_access 53	80	155.1 .60	36190	61.185.215.176	01/22/03 10:38 PM
22	10017	Root_exe_access 53	80	155.1 .60	36190	61.185.215.176	01/22/03 10:38 PM
23	10017	IIS_CGI_Double_Dec	80	155.1 .60	35929	61.185.215.182	01/22/03 10:38 PM
24	10017	IIS_CGI_Double_Dec	80	155.1 .60	36610	61.185.215.188	01/22/03 10:38 PM
25	10017	IIS_CGI_Double_Dec	80	155.1 .60	36724	61.185.215.188	01/22/03 10:38 PM
26	10017	IIS_CGI_Double_Dec	80	155.1 .60	26978	61.185.215.182	01/23/03 12:28 AM


Attack Type Trend Analysis
25
20
15
10
5
0
May
Aug
Nov
Back Orifice
Buffer Overflow
DoS
HTTP Cold Fusion
Intrusion/Compromise
IP Frag Attack
IP Half Scans
Large ICMP Packet
Mail Bomb
Malicious Email
Modified Loki ICMP Tunneling
Mountd Portmap
Net Sweep Echo
Ping Flood
Queso Sweep
Root Kit
RPC Dump
Satan
Source Route Attack
Spam
TCP Conn Req
TCP SYN Port Sweep
TCP SYN/FIN Host Sweep
Tribe Flood/Straceldrat Trojan
Vulnerability Scan
Web Vulnerability Scan
Windows Redbutton Attack
Xterm Display Attack


Attack Origin Trend Analysis
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
70
60
50
40
30
20
10
0
Totals
US
United Kingdom
Ukraine
Taiwan
Switzerland
Sweden
Spain
South Africa
Russia
Romainia
Poland
Peru
Pakistan
New Zealand
Netherlands
Mexico
Malta
Malaysia
Luxembourg
Lichtenstein
Korea
Japan
Italy
Ireland
Hungary
Hong Kong
Greece
Germany
Denmark
Czech Republic
China
Canada
British Columbia
Brazil
Belgium
Australia
May
Jul
Sep
Nov

IDS Deployment Options

- Do nothing
- Deploy with a “kinda sorta” strategy
- Invest in and build “best in class”;
  - People
  - Technology
  - Processes
  - Procedures
  - Training
  - Redundancy
- Outsource / Out-task
  - Recognized “best in class” vendor
  - Brand “X”
- Co-Manage
  - Short term or Long term
  - Recognized “best in class” vendor
  - Brand “X”

Concluding Thoughts

Security and privacy are really business issues with real business impacts.

Effective security and privacy is a process that is built on documented, solid, understandable, and well communicated policies.

Security and privacy can not be obtained solely through tools or technology because it is a moving target and there are no "silver bullets".

Customer trust is based on Security, Privacy, and Communication.