Adv Security and Network Forensics

SIEM

Author: Prof Bill Buchanan

Edinburgh Napier UNIVERSITY

Data increases every day:

- 12TB of Tweets.
- 90% of all data in the Cloud produced in the last two years.
- 2,500,000,000,000,000 bytes of data produced every data 2.5 Quintillion Bytes – 1 billion hard disks

It's part of every aspect of our lives...

Why Computing?

Everything Is dependent on the Internet

- Banking.
- Oil and Gas.
- E-Commerce.
- Transport.
- … virtually everthing

It's all going digital:

- Data.
- Voice.
- Video.
- Sensors.

Firefox | timechart | Get the tutorial data into Splunk | Use fields to search | syslog screen shot kiwi - Google Search | Data scientists are the new rock stars ...

eefutureconnections.economist.com/data-scientists-new-rock-stars-big-data-demands-big-talent/

Most Visited | Getting Started | Suggested Sites | Web Slice Gallery

More from The Economist | Subscription | Log in or register

The Economist

World politics | Business & finance | Economics | Science & technology | Culture | Blogs | Debate | Multimedia | Print edition

Advertisement feature >>

EE: Future Connections

Discover How to Achieve True Mobility For Your Business

HOME | LATEST TOPIC: Superfast Mobility | ABOUT EE | OTHER TOPICS

Data scientists are the new rock stars as big data demands big talent

Written by Olaf Swantee, chief executive officer of EE.

How big is 'big data'? Scratch the surface and the figures will blow your mind. A study at the end of 2012 by IDC predicts the 'digital universe' will reach 40 zettabytes – that's 40,026 gigabytes – by 2020, a 50-fold growth in a decade.

This tidal wave of data will be created by many forces from financial transactions, medical records, mobile phones and social media to the Internet of Things, where everyday machines and objects will be connected to the internet and capable of generating data.

The value for business and society will come from the ability to make sense of this mass

The Economist

Articles from *The Economist*

Driving Transformative Business Strategy

Personal Technology at work: ITs Arab spring

People are demanding to use their own gadgets in their jobs. Trying to thwart them is futile

Bigger Data

How do smartphones reveal shoppers' movements?

NORDSTROM, an American fashion retailer, is known for its high-touch customer service, which has engendered customer loyalty

Driving Transformative Business Strategy

The future of

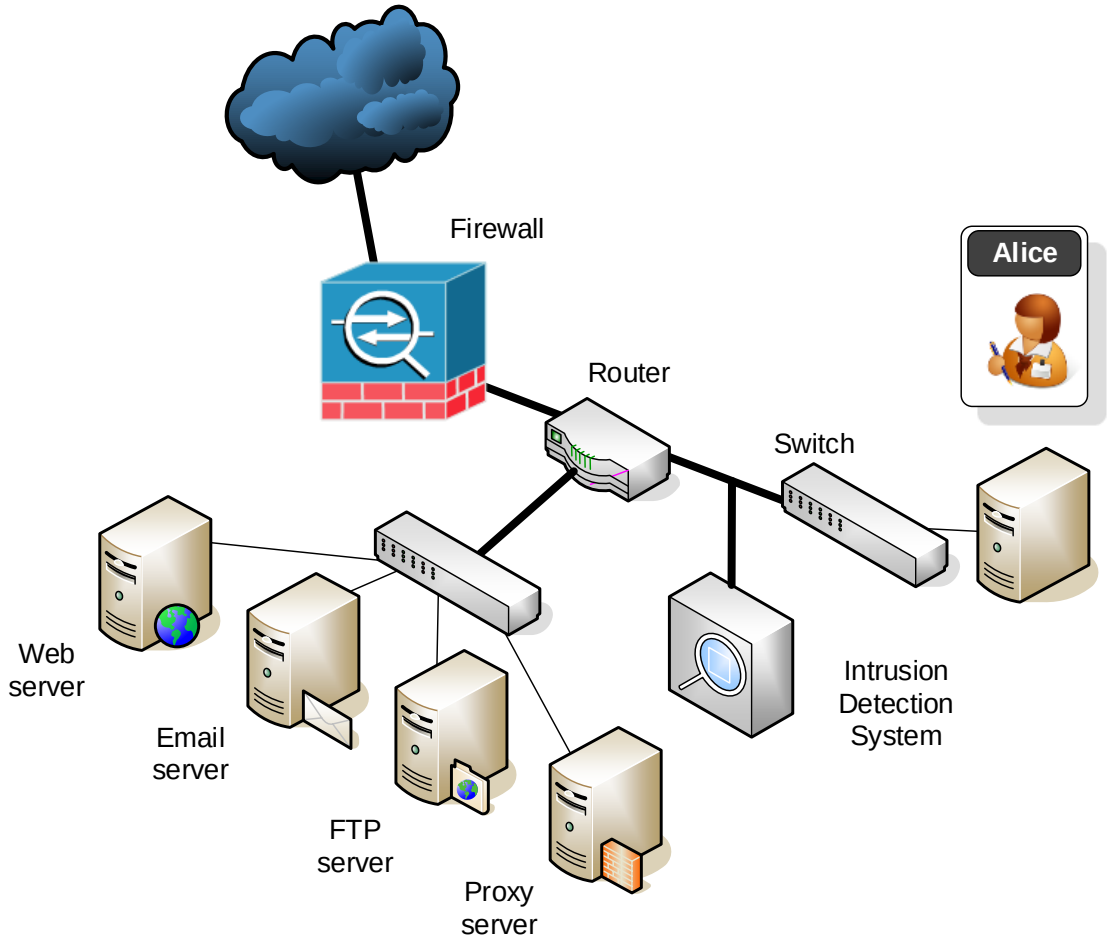
7:34 AM 25-Mar-14

V- Velocity
[Speed of data generation]

V- Variety
[Different forms of data]

V- Veracity
[Trustworthiness]

V- Volume
[Scale of data]



Management report

Sales analysis

Targeted marketing

Trending/Correlation

SIEM

Network Security

2011: Watson beats humans at Jeopardy!

1997: Deep Blue deep Kasparov

2013: Watson beats Cancer Specialists

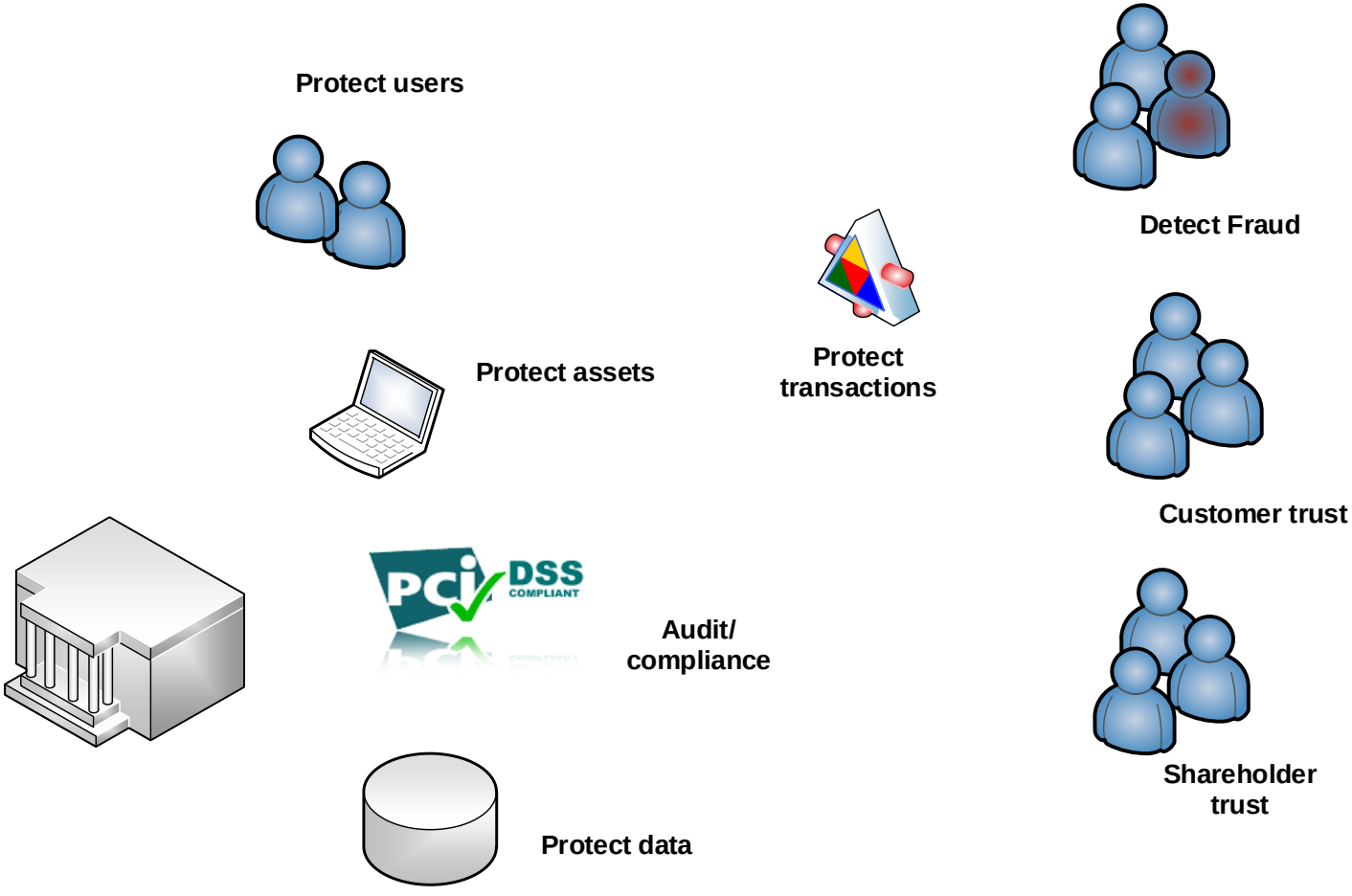
Adv Security and Network Forensics

SIEM

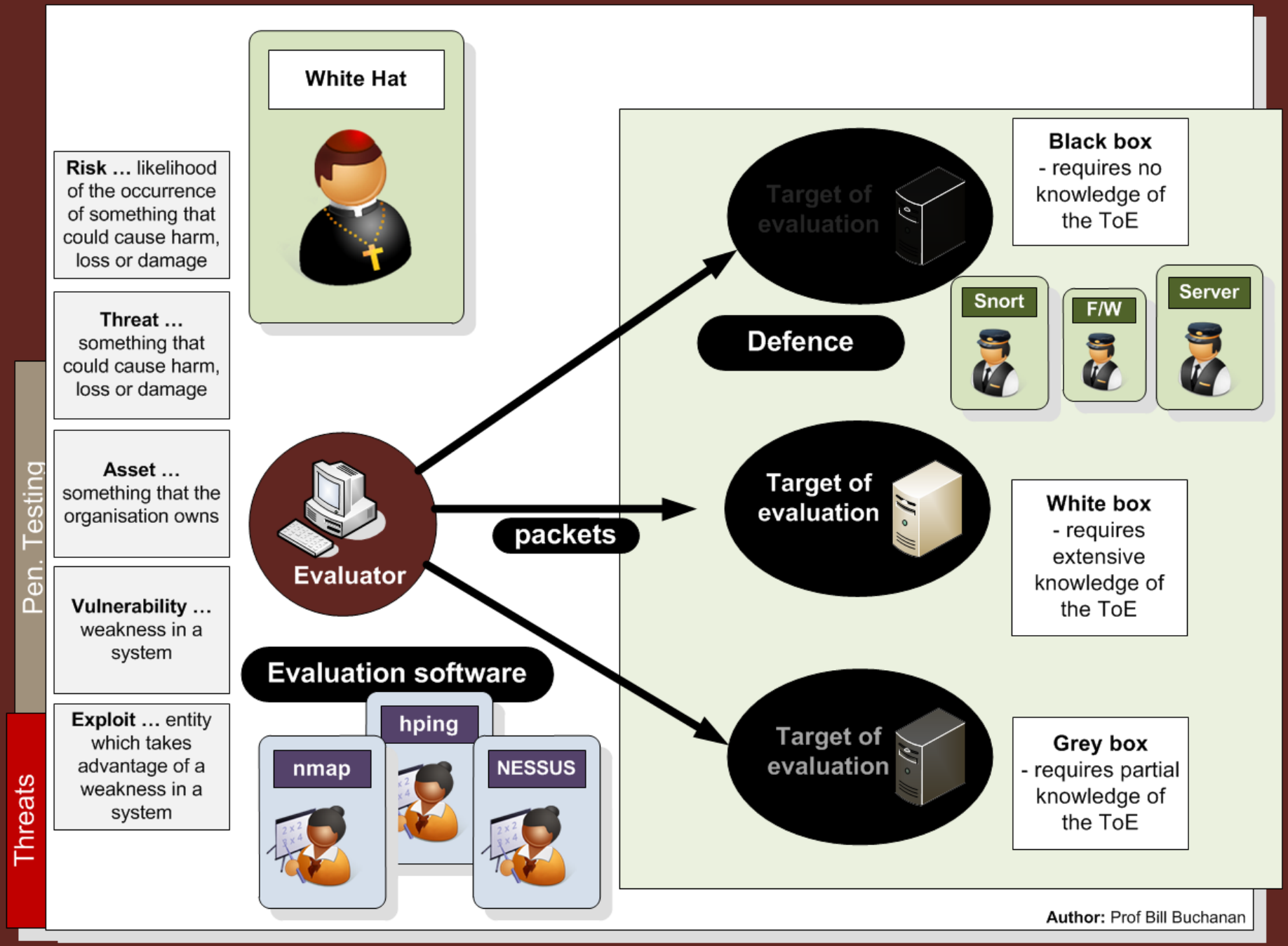
Author: Prof Bill Buchanan

SIEM

Network Security



Why?



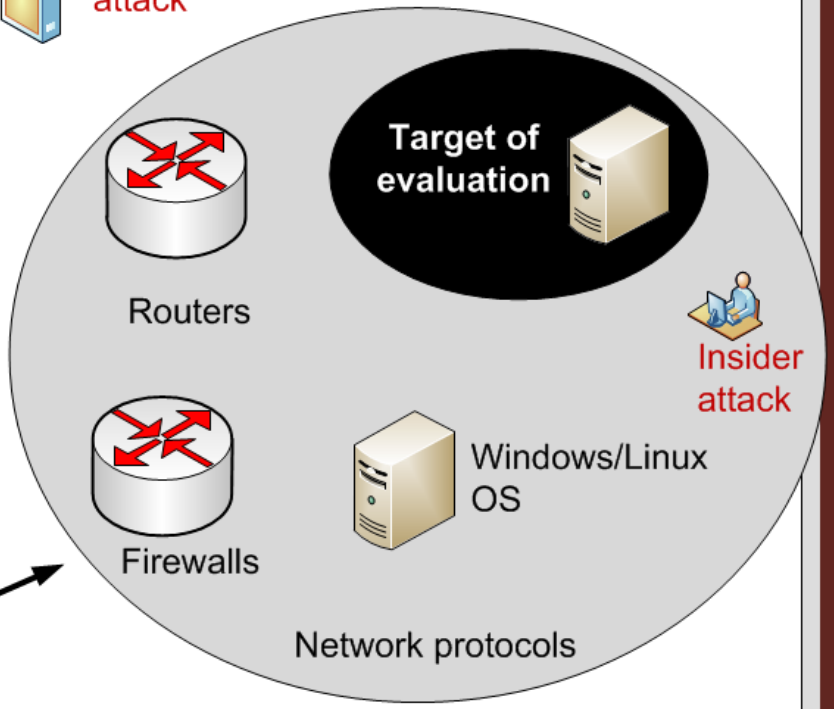
White, grey and black box testing

Code of Ethics

- Do not exceed authorization limits
- Be ethical
- Limit possible damage
- Maintain confidentiality

Stolen equipment attack

Social engineering



Insider attack

Level I

High-level testing – does not include a hands-on test

Physical entry attack

Level II

Network Evaluation - information gathering, scanning and vulnerability assessment scanning

Level III

Pen Testing - taking on an adversarial role

Outsider attack

Pen. Testing

Threats

Author: Prof Bill Buchanan

Levels of testing

Confidentiality

- Only authorized entities can access sensitive data

C

Locked doors
Armed guards
Fences
Firewalls
Passwords
Encryption
VPN Access

Access control
Windows File Protection
MD5 checksum
SHA-1 checksum
Network Operating System

Integrity

- Changes data by unauthorized entities is detected.
- Only authorized entities can change sensitive data

I

C

I

A

Target of evaluation

Availability

- Only authorized entities have continual access to data

A

Failover equipment
Mirror servers

Pen. Testing

Threats

Author: Prof Bill Buchanan

Code of Ethics

- Do not exceed authorization limits
- Be ethical
- Limit possible damage
- Maintain confidentiality

Pen. Testing

Threats

Written permission from the organisation.

Scope the project

Perform the assessment

Post assessment activities

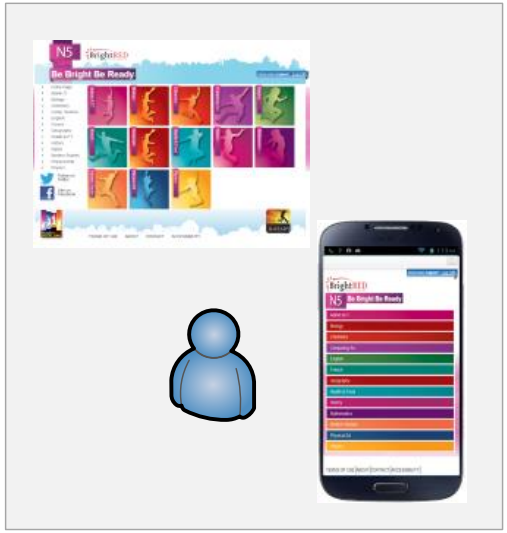
Why?

- **Gramm-Leach-Bliley Act** (US reg to allow banks, security firms and insurance companies to merge/share data)
- **US Health Insurance Portability and Accountability Act (HIPAA)**.
- **Security and Freedom through Encryption (SAFE)**. define the rights of US Citizens to the use of encryption without key escrow.
- **Computer Fraud and Abuse Act**. Reduce hacking by defining penalties against incidents.
- **Privacy Act of 1974**. Respects the rights of the individual unless permission is given.
- **Federal Information Security Management Act (FISMA)**. Aims to strengthen US federal government security by the use of yearly audits.
- **Economic Espionage Act of 1996**. Aims to criminalise the misuse of trade secrets.
- **Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT)**. Permits the government to monitor hackers without a warrant.
- **Sarbanes-Oxley (SOX) Act**. Relates to transparent account and reporting of companies

Author: Prof Bill Buchanan

Risk 4: One Password Fits All

Edinburgh Napier UNIVERSITY



Adobe

150 million accounts compromised

#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	123456
2.	446162	j9p+HwtWWT86aMjgZFLzYg==	123456789
3.	345834	L8qbAD3jl3jioxG6CatHBw==	password
4.	211659	BB4e6X+b2xLioxG6CatHBw==	adobe123
5.	201580	j9p+HwtWWT/ioxG6CatHBw==	12345678
6.	130832	5djv7ZCI2ws=	qwerty
7.	124253	dQi0asWPYvQ=	1234567
8.	113884	7LqYzKVeq8I=	111111
9.	83411	PMDTbP0LZxu03SwrFUvYGA==	photoshop
10.	82694	e6MPXQ5G6a8=	123123

TJ-maxx Marshalls

47 million accounts

LinkedIn

6.5 million accounts (June 2013)

Windows Live

One account hack … leads to others

1 million accounts – in plain text. 77 million compromised

Dropbox compromised 2013

citigroup

200,000 client accounts

SIEM

Network Security

Build and Maintain and Secure Network
Firewall. System passwords.

Protect Cardholder Data
Stored cardholder data. Encrypt data.

Monitor and Test Networks
Track/monitor accesses. Perform security tests.

Maintain Vulnerability Management Program
Anti-virus. Develop/ maintain secure systems and apps.

Define/Maintain Security Policy
Design and implement a policy which focuses on security.

Strong Access Control
Restrict access to cardholder data. Assign unique ID for each user who accesses. Restrict physical access.

Enron, Tyco International, Adelphia, Peregrine Systems and WorldCom. U.S. Senator Paul Sarbanes and U.S. Representative Michael G. Oxley. USA, Canada, France, etc.

Public Company Accounting Oversight Board

Analyst Conflicts of Interest

Auditor Independence

Corporate Responsibility

Corporate Tax Returns

SIEM

Network Security

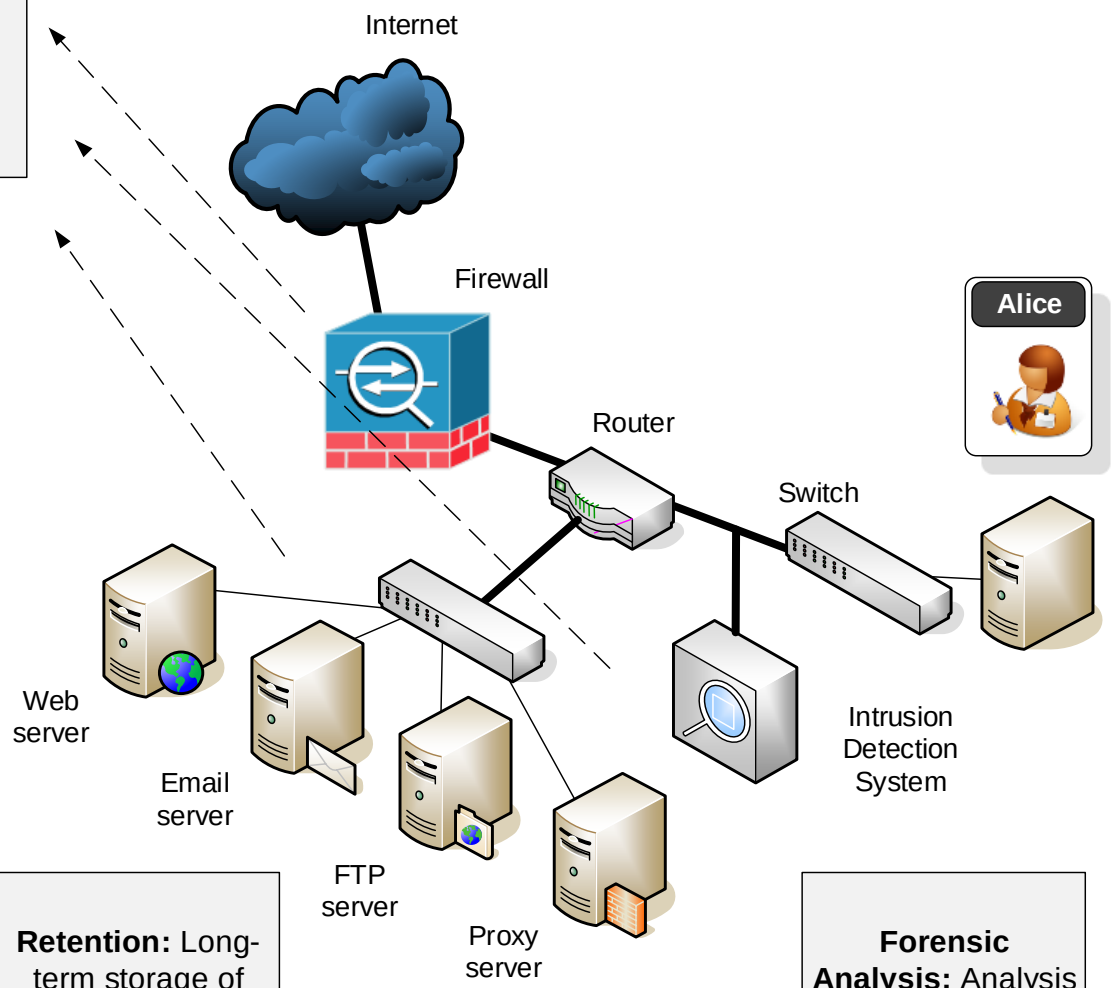
SOX

Log Aggregation: Data from many sources … networks, databases, applications, servers, etc

Correlation: Links events together into a coherent instances (time-lining)

Dashboard: Provides an overview of events and alerts for analysis/response

Complaince: Gathering and reporting of audit/ compliance (PCI-DSS, etc).



Retention: Long-term storage of data for audit/ compliance

Forensic Analysis: Analysis of logs across infrastructure

SIEM

Network Security

SIEM

Network Security

Local host logs
- Application.
- Security.
- System
- etc

File and Directories
- CRUD.
- Security changes.

Performance
- CPU.
- Memory.
- Threads.

Database Access
- Logs.

TCP/UDP
- Syslog.

Remote Access
- Logs.

Registry Monitoring
- Key changes.
- Updates.

Environmental
- Temp.
- Humidity.

Active Directory
- User additions.
- Host changes.
- Logins

Intrusion Detection
- Alerts

Email
- Logs.

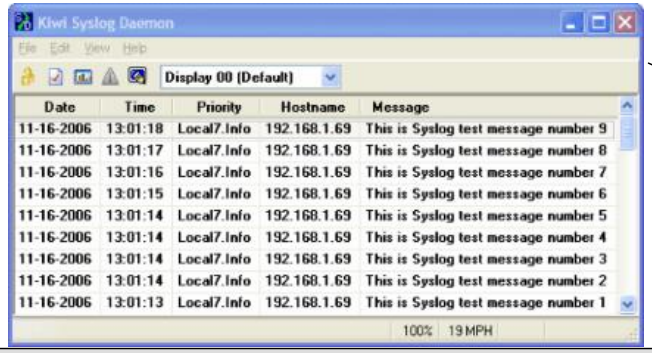
Print Monitoring
- Jobs.

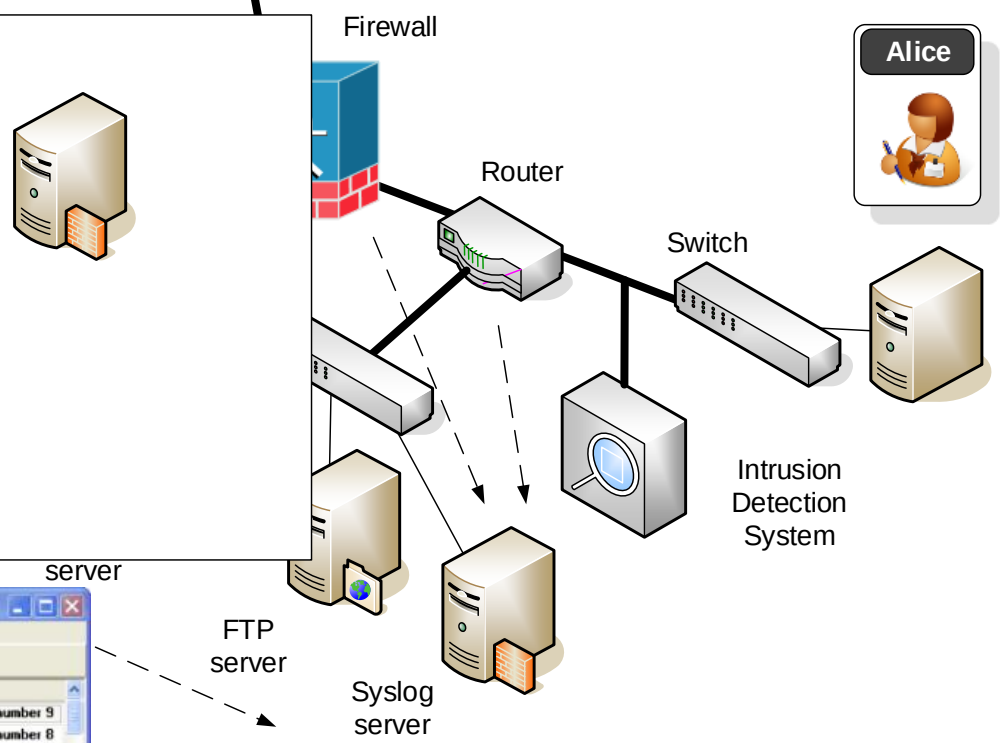
Logs

Buffered logging:

0	Emergencies	System shutting down due to missing fan tray
1	Alerts	Temperature limit exceeded
2	Critical	Memory allocation failures
3	Errors	Interface Up/Down messages
4	Warnings	Configuration file written to server, via SNMP request
5	Notifications	Line protocol Up/Down
6	Information	Access-list violation logging
7	Debugging	Debug messages

```
> enable
# config t
(config)# logging on
(config)# logging 212.72.52.7
(config)# logging buffer 440240
(config)# logging trap emergency
(config)# logging monitor emergency
(config)# logging console emergency
(config)# logging buffer emergency
(config)# clock timezone AKDT
```





SIEM

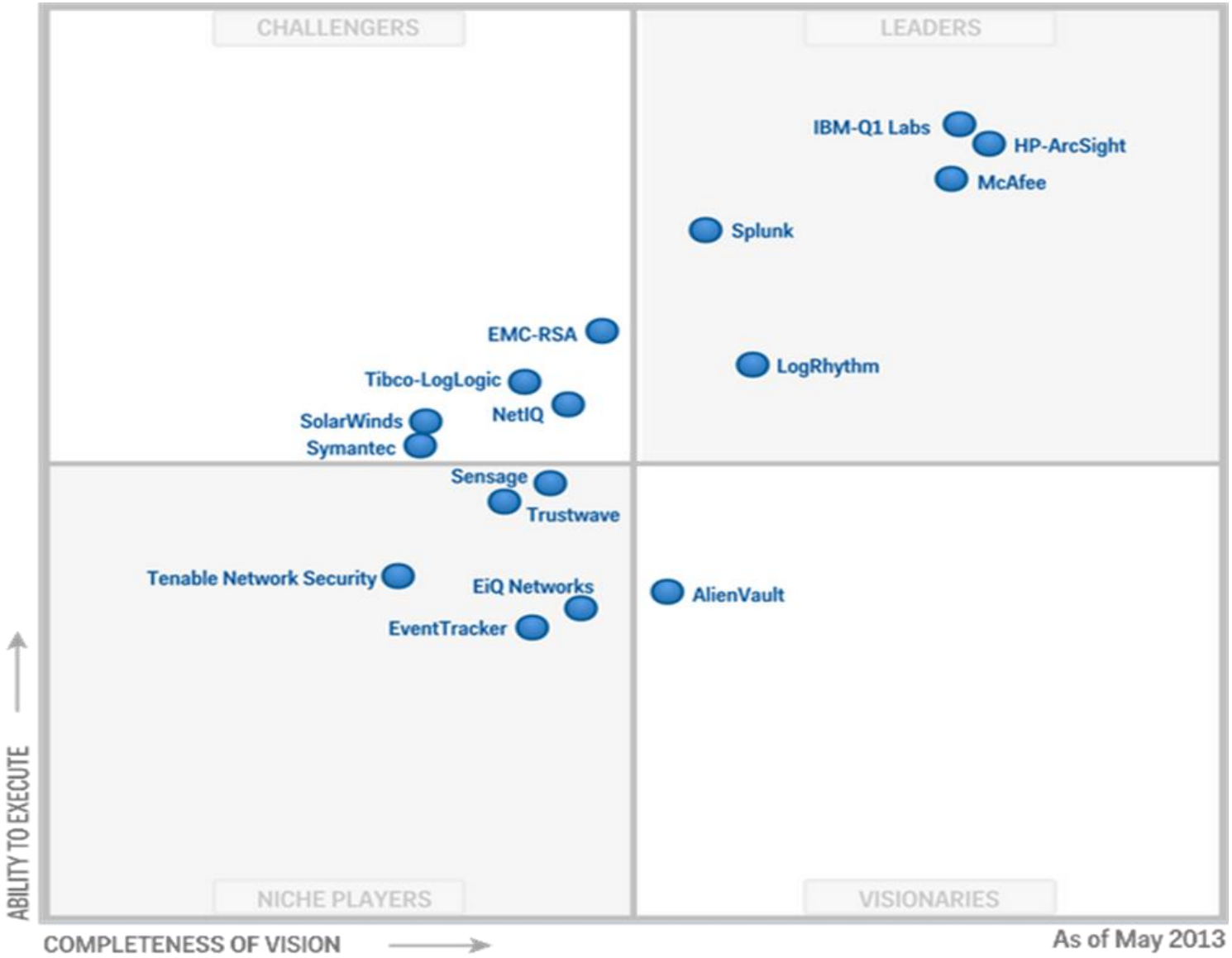
Network Security

Syslog

SIEM

Types

Author: Prof Bill Buchanan

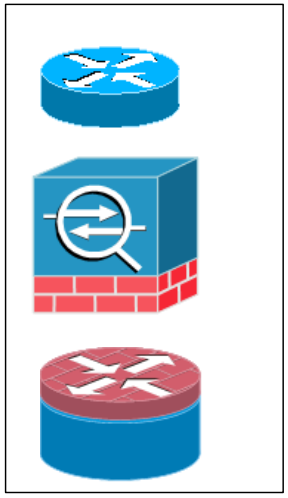


SIEM

Network Security

SIEM

Network Security

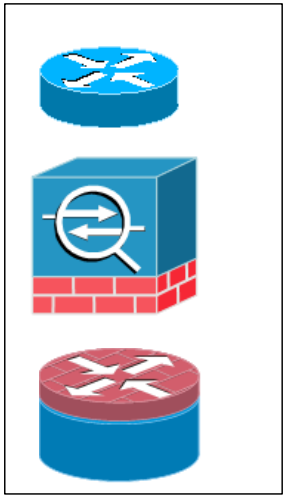


Data collected with Cisco NetFlow

```
Router# configure terminal
// Destination is 192.168.1.1 UDP Port: 999
Router(config)# ip flow-export destination 192.168.1.1 999
Router(config)# ip flow-export version 9
Router(config)# interface ethernet 0/0
// Monitor incoming
Router(config-if)# ip flow ingress
```

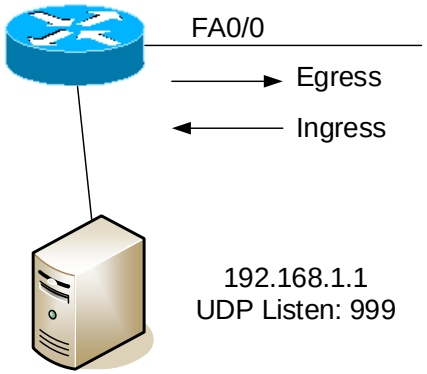
SIEM

Network Security



Data collected with Cisco NetFlow

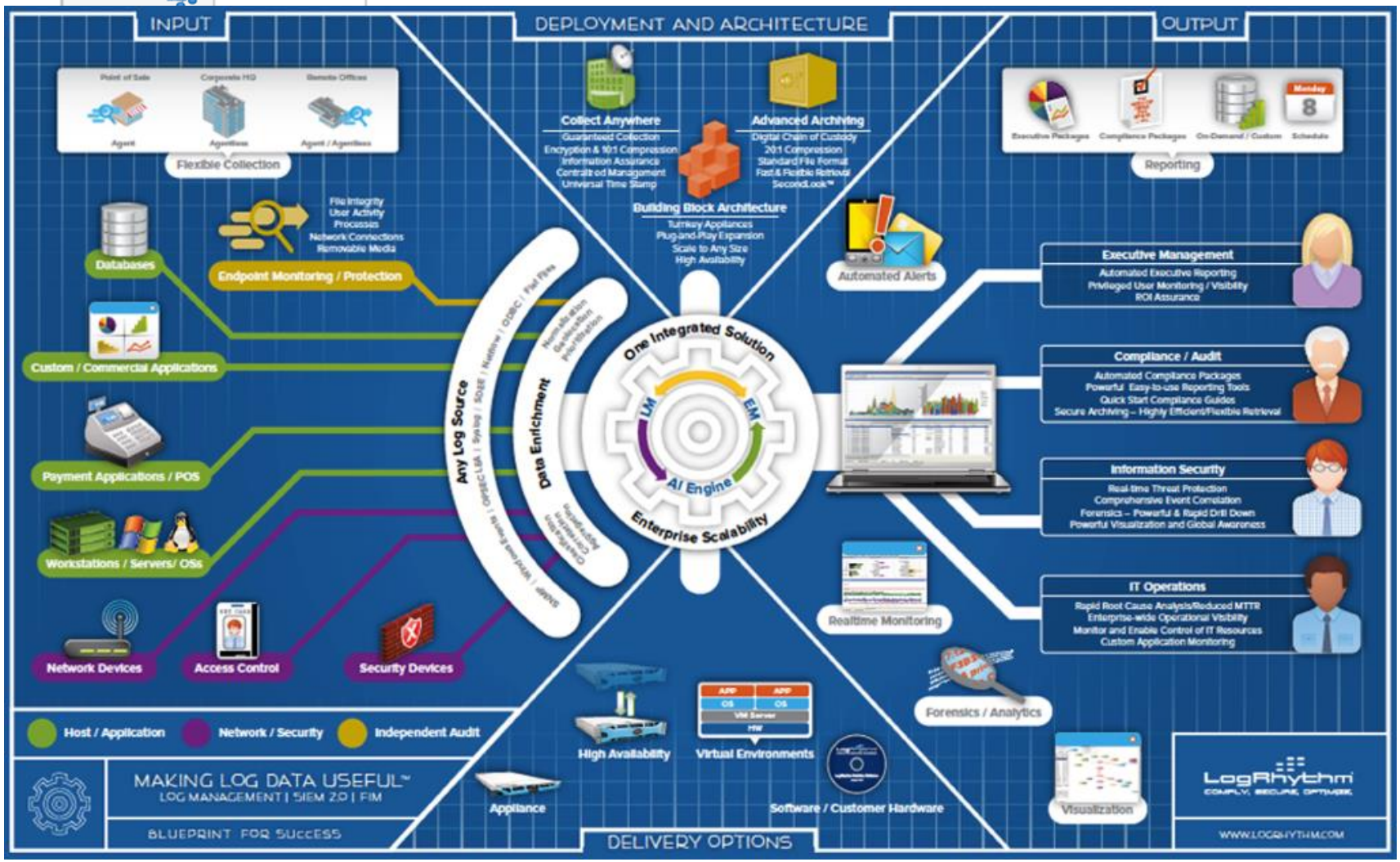
NetFlow Route



NetFlow Collection Agent

```
Router# show ip cache flow
IP packet size distribution (1103746 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .249 .694 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .027 .000 .027 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  35 active, 4061 inactive, 980 added
  2921778 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-FTP            108       0.0      1133    40      2.4    1799.6       0.9
TCP-FTPD           108       0.0      1133    40      2.4    1799.6       0.9
TCP-WWW             54       0.0      1133    40      1.2    1799.6       0.8
TCP-SMTP            54       0.0      1133    40      1.2    1799.6       0.8
TCP-BGP             27       0.0      1133    40      0.6    1799.6       0.7
TCP-NNTP            27       0.0      1133    40      0.6    1799.6       0.7
TCP-other          297       0.0      1133    40      6.8    1799.7       0.8
UDP-TFTP            27       0.0      1133    28      0.6    1799.6       1.0
UDP-other          108       0.0      1417    28      3.1    1799.6       0.9
ICMP               135       0.0      1133   427      3.1    1799.6       0.8
Total:             945       0.0      1166    91     22.4    1799.6       0.8
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.67.6    Et1/0.1       172.16.10.200   01 0000 0C01    51
Et0/0         10.10.18.1      Null          172.16.11.5     11 0043 0043    51
Et0/0         10.10.18.1      Null          172.16.11.5     11 0045 0045    51
Et0/0         10.234.53.1     Et1/0.1       172.16.10.2     01 0000 0800    51

.
.
Et0/0         172.16.1.84     Et1/0.1       172.16.10.19    06 0087 0087    50
Et0/0         172.16.1.84     Et1/0.1       172.16.10.19    06 0050 0050    51
Et0/0         172.16.1.85     Et1/0.1       172.16.10.20    06 0089 0089    49
Et0/0         172.16.1.85     Et1/0.1       172.16.10.20    06 0050 0050    50
Et0/0         10.251.10.1     Et1/0.1       172.16.10.2     01 0000 0800    51
Et0/0         10.162.37.71    Null          172.16.11.3     06 027C 027C    49
```

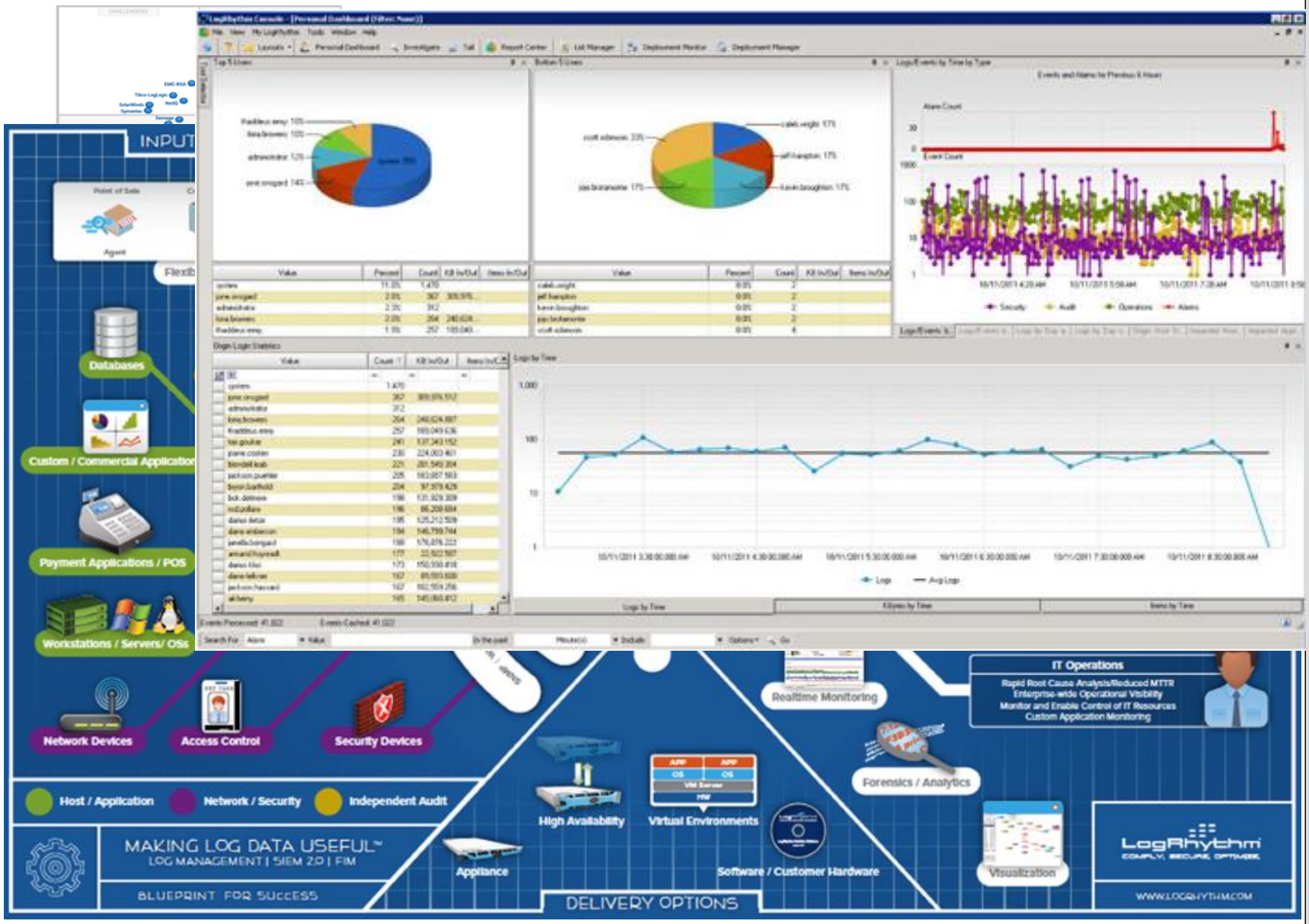


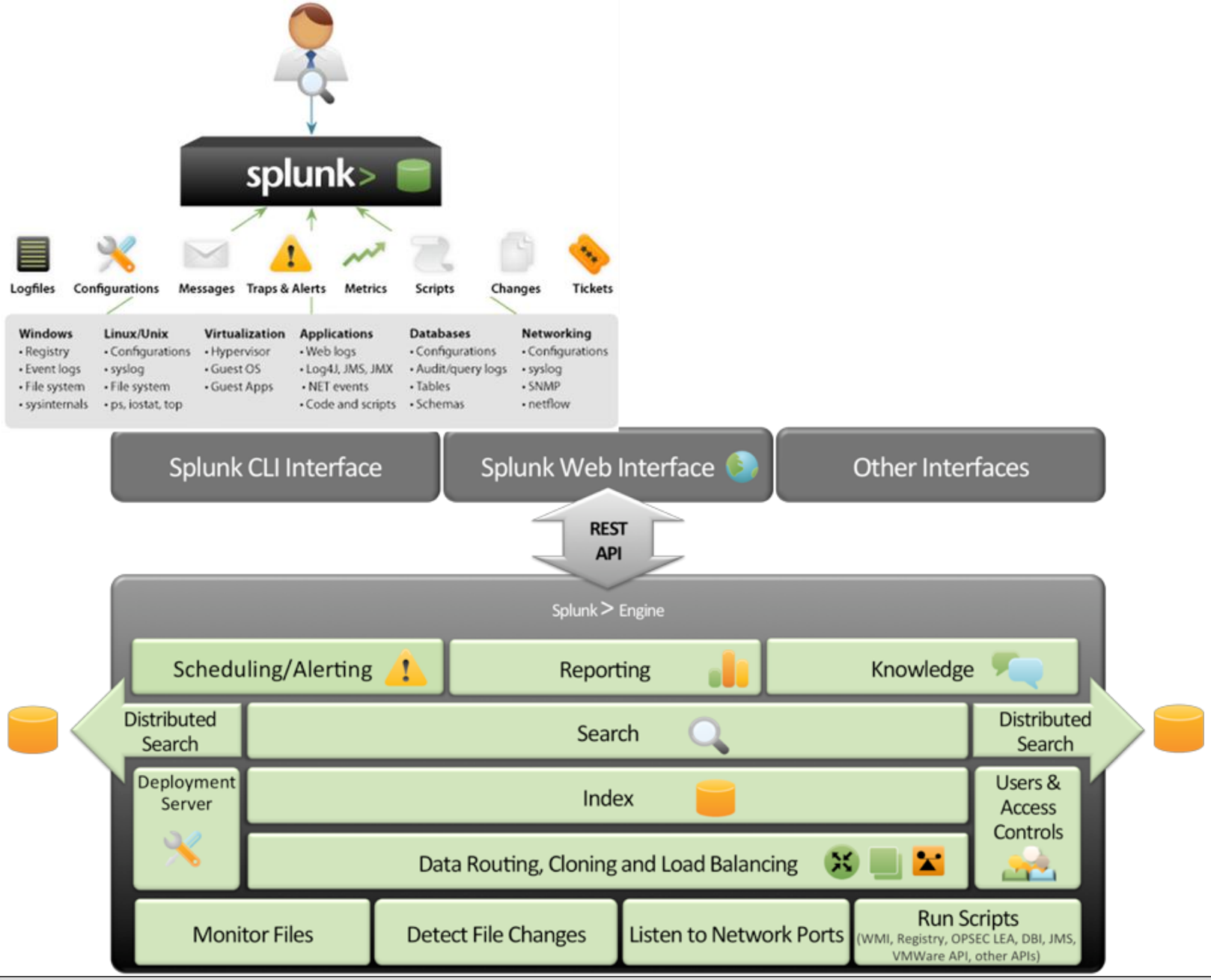
SIEM

Network Security

SIEM

Network Security





SIEM

Network Security

SIEM

Network Security

Top Activity by Pool Name, Last 24 Hrs

Splunk manual usage

Total kb's indexed by sourcetype

Messages recieved per client IP

Recent packet retransmits

CPU utilization of Splunk processes

HTTP status received, past 60 minutes (other than 200)

Data Routing, Cloning and Load Balancing

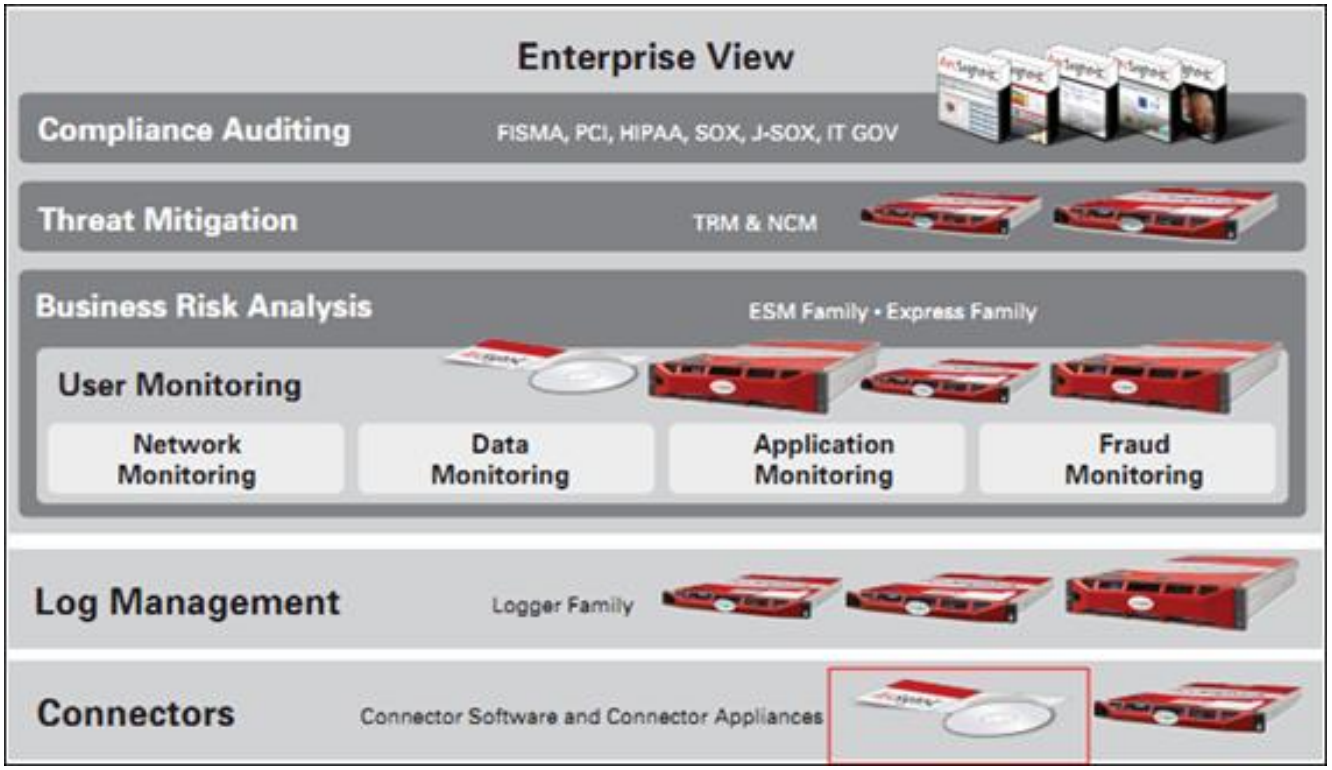
Access Controls

Monitor Files

Detect File Changes

Listen to Network Ports

Run Scripts
(WMI, Registry, OPSEC LEA, DBI, JMS, VMWare API, other APIs)



SIEM

Network Security

ArcSight Logger

EPS In: 91
EPS Out: 0
CPU Load: 5%

Help
About
Options
Logout

Monitor | Analyze | Reports | Configuration | System Admin | admin

Last 10 minutes

Search: OSSEC

Go!

Advanced Search

Fields: All Fields | Auto Update: 5 min | 7 | 54,777 | 00:02.142 | Export Results...

1 bar = 5 second

21:12:16 21:12:56 21:13:36 21:14:16 21:14:56 21:15:36 21:16:16

Events

	Time (Event Time)	Device	Logger	deviceVendor	deviceProduct	deviceVersion	deviceEventClassId	name	deviceAddress	deviceCustomS
1	2011/05/11 21:12:16 CEST	10.0.20.10	Local	Trend Micro Inc.	OSSEC HIDS	v2.5.1	5302	User missed the password to	ubuntusvr	ubuntusvr->;/va
2	2011/05/11 21:12:30 CEST	10.0.20.10	Local	Trend Micro Inc.	OSSEC HIDS	v2.5.1	5302	User missed the password to	ubuntusvr	ubuntusvr->;/va
3	2011/05/11 21:13:42 CEST	10.0.20.10	Local	Trend Micro Inc.	OSSEC HIDS	v2.5.1	5302	User missed the password to	ubuntusvr	ubuntusvr->;/va
4	2011/05/11 21:16:38 CEST	10.0.20.10	Local	Trend Micro Inc.	OSSEC HIDS	v2.5.1	5302	User missed the password to	ubuntusvr	ubuntusvr->;/va
5	2011/05/11 21:16:38 CEST	10.0.20.10	Local	Trend Micro Inc.	OSSEC HIDS	v2.5.1	5301	User missed the password to	ubuntusvr	ubuntusvr->;/va
6	2011/05/11 21:16:38 CEST	10.0.20.10	Local	Trend Micro Inc.	OSSEC HIDS	v2.5.1	5710	Attempt to login using a non-e:	ubuntusvr	ubuntusvr->;/va
7	2011/05/11 21:16:38 CEST	10.0.20.10	Local	Trend Micro Inc.	OSSEC HIDS	v2.5.1	502	Ossec server started.	ubuntusvr	ubuntusvr->;oss

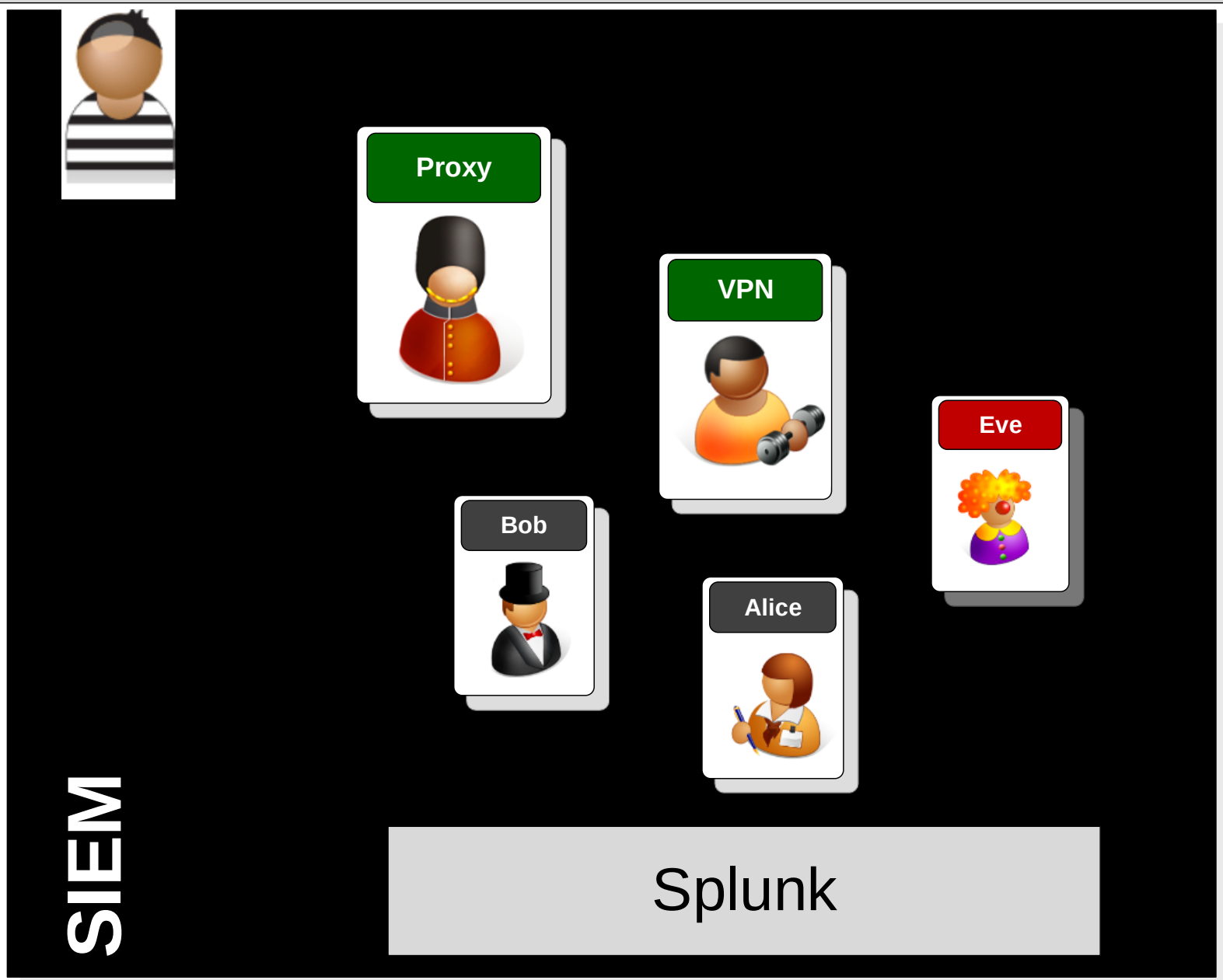
Page 1 of 1 | Show RAW: All None | Displaying 1 - 7 of 7

Log Management — Logger Family

Connectors — Connector Software and Connector Appliances

SIEM

Network Security



Author: Prof Bill Buchanan

```
209.160.24.63 - - [11/Mar/2014:18:22:16] "GET /product.screen?productId=WC-SH-A02&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 3878 "http://www.google.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 349

209.160.24.63 - - [11/Mar/2014:18:22:16] "GET /oldlink?itemId=EST-6&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 1748 "http://www.buttercupgames.com/oldlink?itemId=EST-6" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 731

209.160.24.63 - - [11/Mar/2014:18:22:17] "GET /product.screen?productId=BS-AG-G09&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 2550 "http://www.buttercupgames.com/product.screen?productId=BS-AG-G09" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 422

209.160.24.63 - - [11/Mar/2014:18:22:19] "POST /
category.screen?categoryId=STRATEGY&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 407 "http://
www.buttercupgames.com/cart.do?action=remove&itemId=EST-7&productId=PZ-SG-G05" "Mozilla/5.0 (Windows NT 6.1;
WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 211

209.160.24.63 - - [11/Mar/2014:18:22:20] "GET /product.screen?productId=FS-SG-G03&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 2047 "http://www.buttercupgames.com/category.screen?categoryId=STRATEGY" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 487
```

Access.log

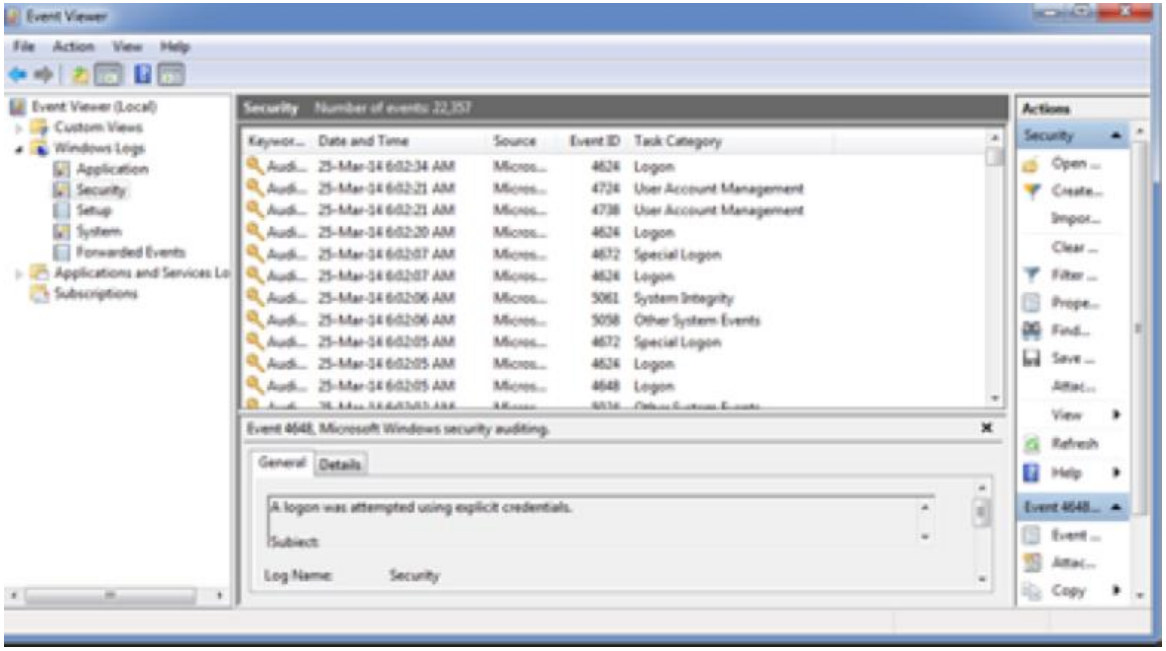
```
#Software: Microsoft Internet Information Services 7.5
#Date: 2014-03-25 00:00:09
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc-substatus sc-win32-status time-taken
2014-03-25 00:00:09 10.185.7.7 GET /ip/whois site=asos.com 80 - 162.244.11.111 Opera/
  9.80+(Windows+NT+6.2;+Win64;+x64)+Presto/2.12.388+Version/12.16 404 0 0 155
2014-03-25 00:00:12 10.185.7.7 GET /security/information/bmp - 80 - 66.249.68.217 Mozilla/5.0+(compatible;+Googlebot/
  2.1;++http://www.google.com/bot.html) 500 19 183 77
2014-03-25 00:00:12 10.185.7.7 GET /ip/whois site=blogspot.nl 80 - 78.46.169.130 Opera/
  9.80+(Windows+NT+6.2;+Win64;+x64)+Presto/2.12.388+Version/12.16 404 0 0 233
2014-03-25 00:00:15 10.185.7.7 GET /Content/footer.png - 80 - 81.133.198.251 Mozilla/
  5.0+(Windows+NT+6.3;+WOW64;+rv:27.0)+Gecko/20100101+Firefox/27.0 404 0 64 5693
2014-03-25 00:00:17 10.185.7.7 GET /ip/whois site=proxyring.com 80 - 110.85.106.101 Opera/
  9.80+(Windows+NT+6.2;+Win64;+x64)+Presto/2.12.388+Version/12.16 404 0 0 14149
2014-03-25 00:00:21 10.185.7.7 GET /ip/whois site=surewest.net 80 - 216.169.139.190 Opera/
  9.80+(Windows+NT+6.2;+Win64;+x64)+Presto/2.12.388+Version/12.16 404 0 0 171
2014-03-25 00:00:23 10.185.7.7 GET / - 80 - 203.206.171.20 Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:27.0)+Gecko/
  20100101+Firefox/27.0 200 0 0 530
```

IIS Log

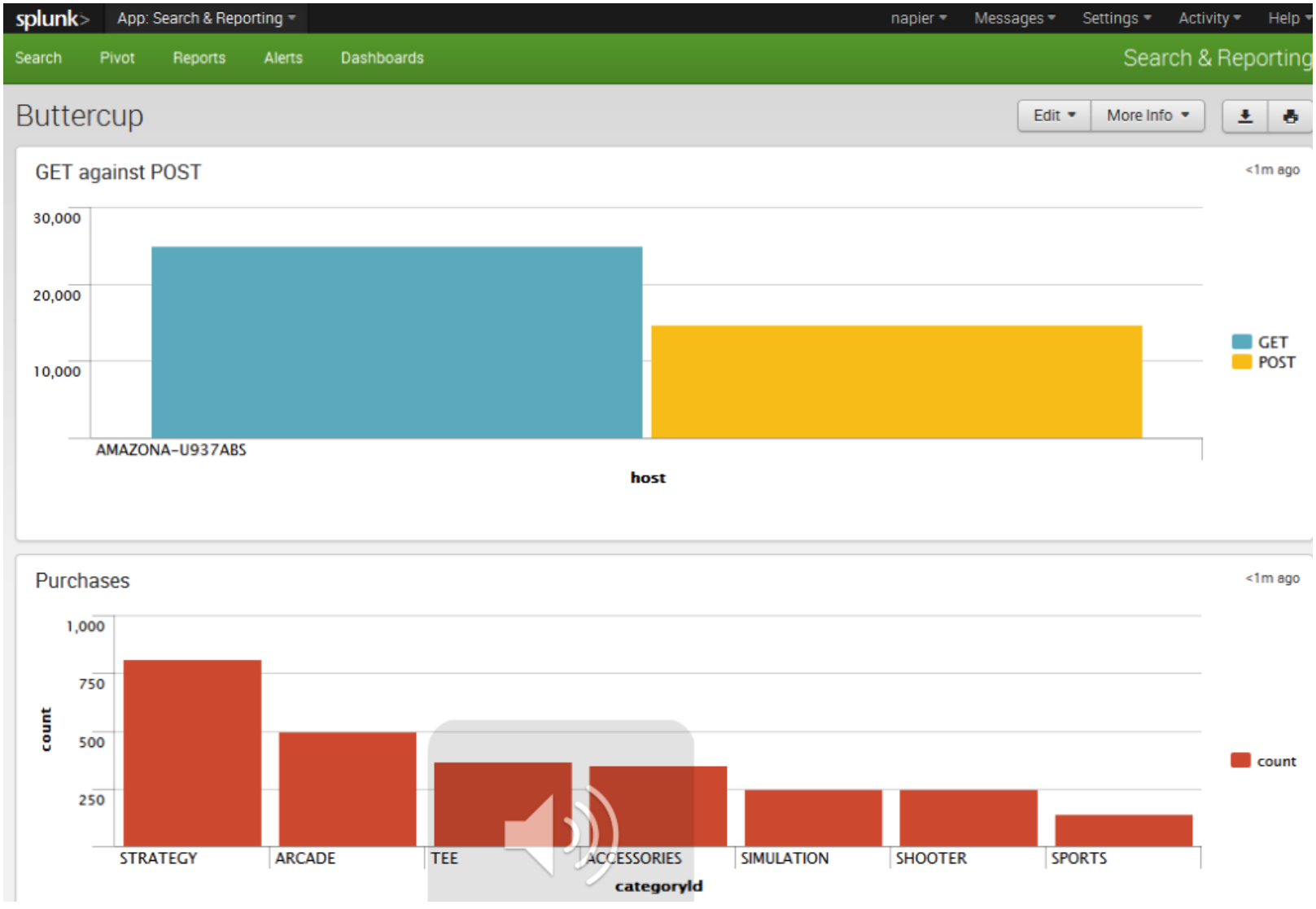
Web logs

```
Thu Mar 11 2014 00:15:01 www1 sshd[4747]: Failed password for invalid user jabber from 118.142.68.222 port 3187 ssh2
Thu Mar 11 2014 00:15:01 www1 sshd[4111]: Failed password for invalid user db2 from 118.142.68.222 port 4150 ssh2
Thu Mar 11 2014 00:15:01 www1 sshd[5359]: Failed password for invalid user pmuser from 118.142.68.222 port 3356 ssh2
Thu Mar 11 2014 00:15:01 www1 su: pam_unix(su:session): session opened for user root by djohnson(uid=0)
Thu Mar 11 2014 00:15:01 www1 sshd[2660]: Failed password for invalid user irc from 118.142.68.222 port 4343 ssh2
Thu Mar 11 2014 00:15:01 www1 sshd[1705]: Failed password for happy from 118.142.68.222 port 4174 ssh2
Thu Mar 11 2014 00:15:01 www1 sshd[1292]: Failed password for nobody from 118.142.68.222 port 1654 ssh2
Thu Mar 11 2014 00:15:01 www1 sshd[1560]: Failed password for invalid user local from 118.142.68.222 port 4616 ssh2
Thu Mar 11 2014 00:15:01 www1 sshd[59414]: Accepted password for myuan from 10.1.10.172 port 1569 ssh2
Thu Mar 11 2014 00:15:01 www1 sshd[1876]: Failed password for invalid user db2 from 118.142.68.222 port 1151 ssh2
Thu Mar 11 2014 00:15:01 www1 sshd[3310]: Failed password for apache from 118.142.68.222 port 4343 ssh2
Thu Mar 11 2014 00:15:01 www1 sshd[2149]: Failed password for nobody from 118.142.68.222 port 1527 ssh2
Thu Mar 11 2014 00:15:01 www1 sshd[2766]: Failed password for invalid user guest from 118.142.68.222 port 2581 ssh2
```

Secure.log



Security log



SIEM

Network Security

Security log

Adv Security and Network Forensics

SIEM

Author: Prof Bill Buchanan