

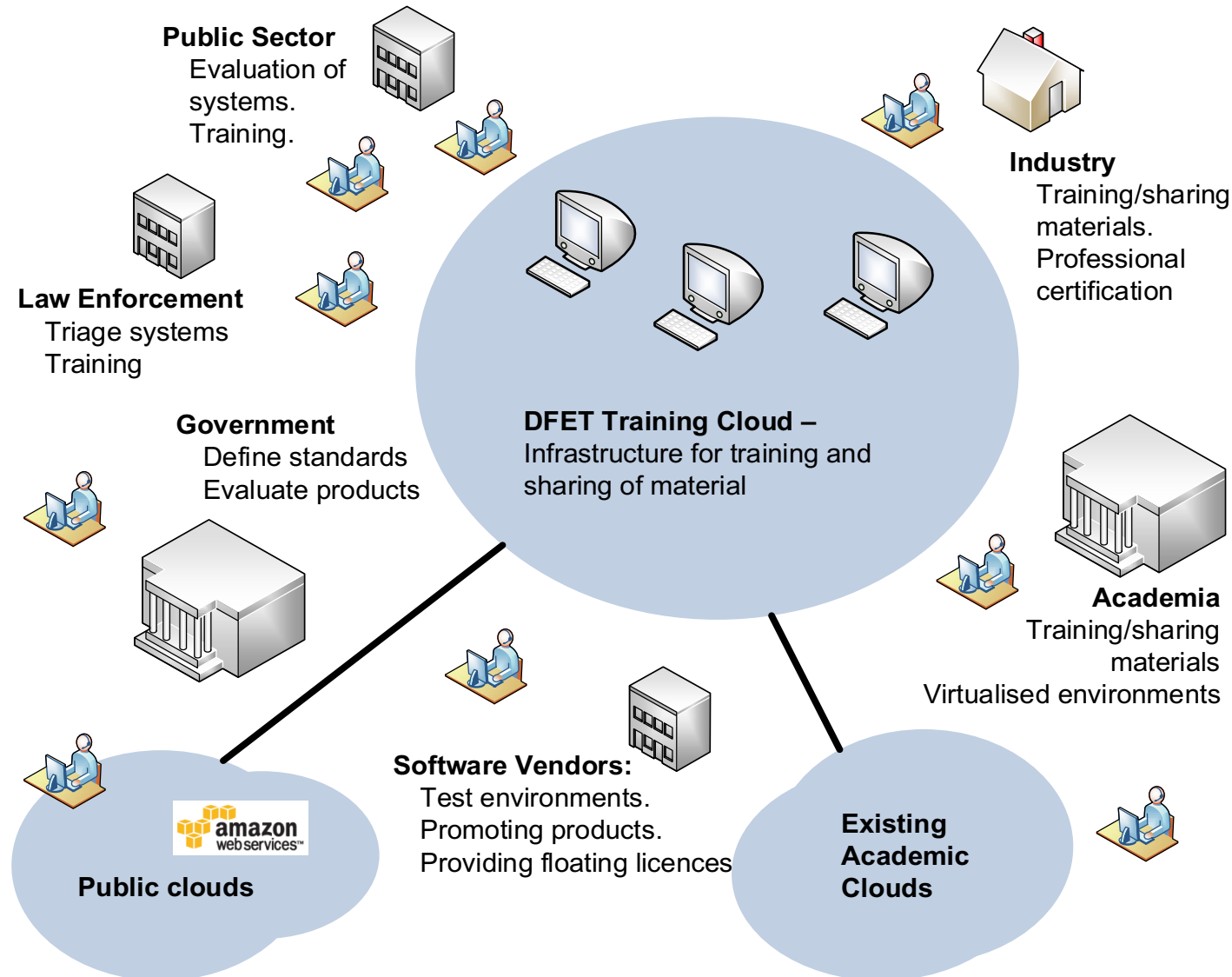


Design and Evaluation of [vSoC]: Virtualised Security Operations Centre

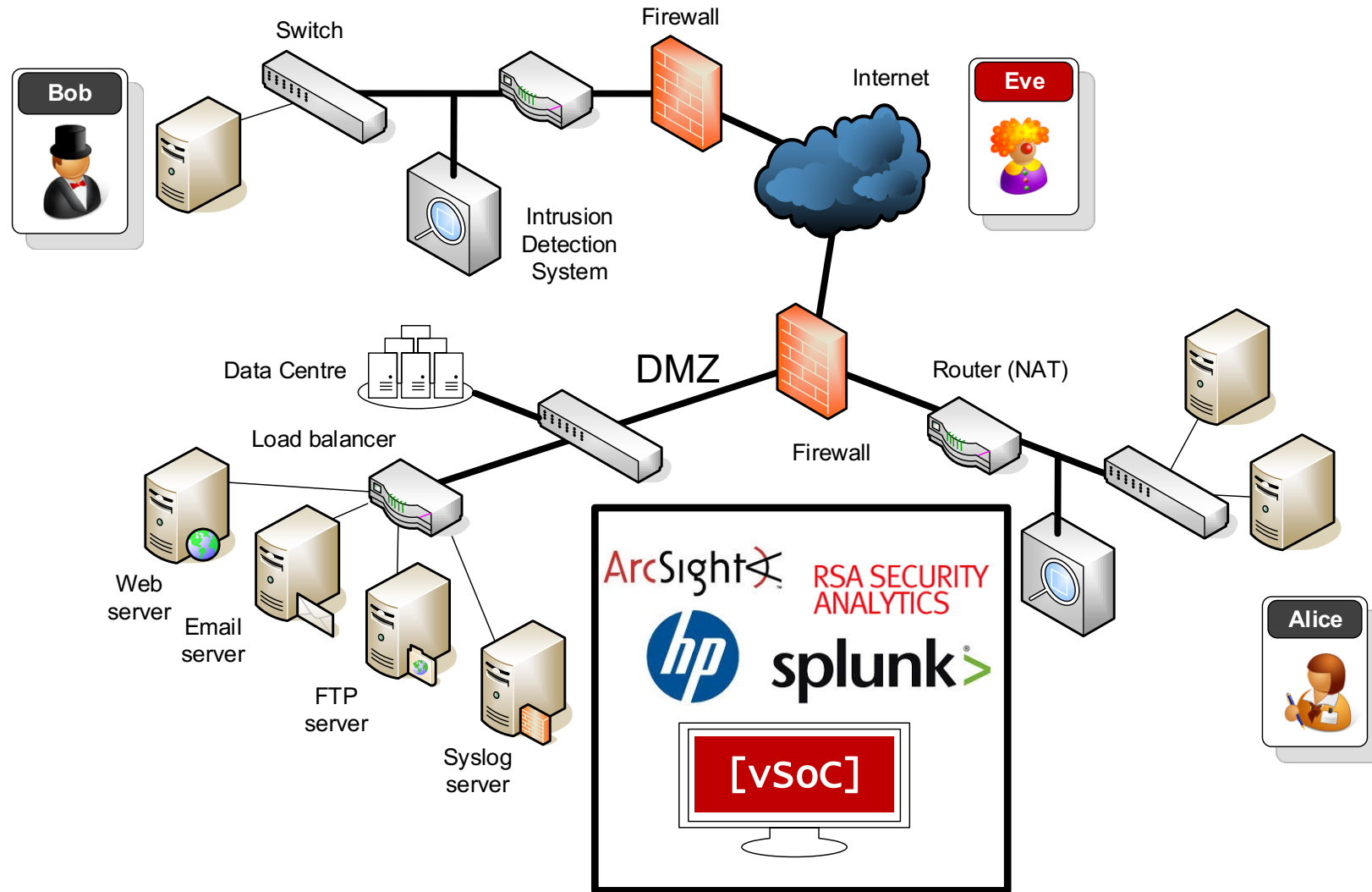
Prof William J Buchanan

<http://thecyberacademy.org>

Sharing of resources



Building vSoC



vSoC/DFET Cloud

The current DFET Cloud contains five main cluster nodes, where each cluster node runs:

- VMware vSphere 5.5 with VMware vCenter used to manage the instances.
- 170GHz CPU, 767GB of memory.
- 40TB of disk space.
- 72 Processors.
- Running over 2,500 running VMs.



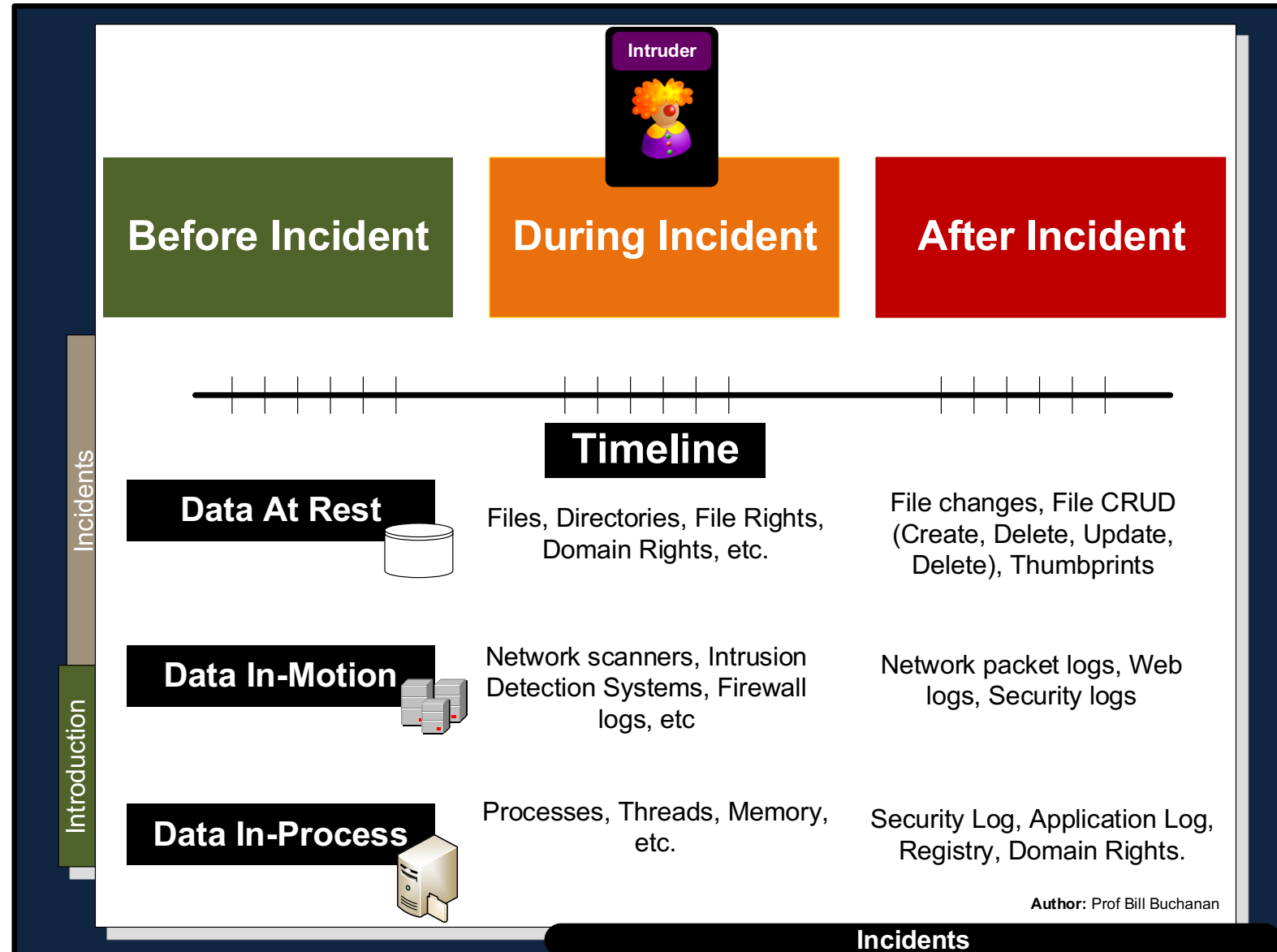


The Move Toward Security Analytics

Big Data/SIEM

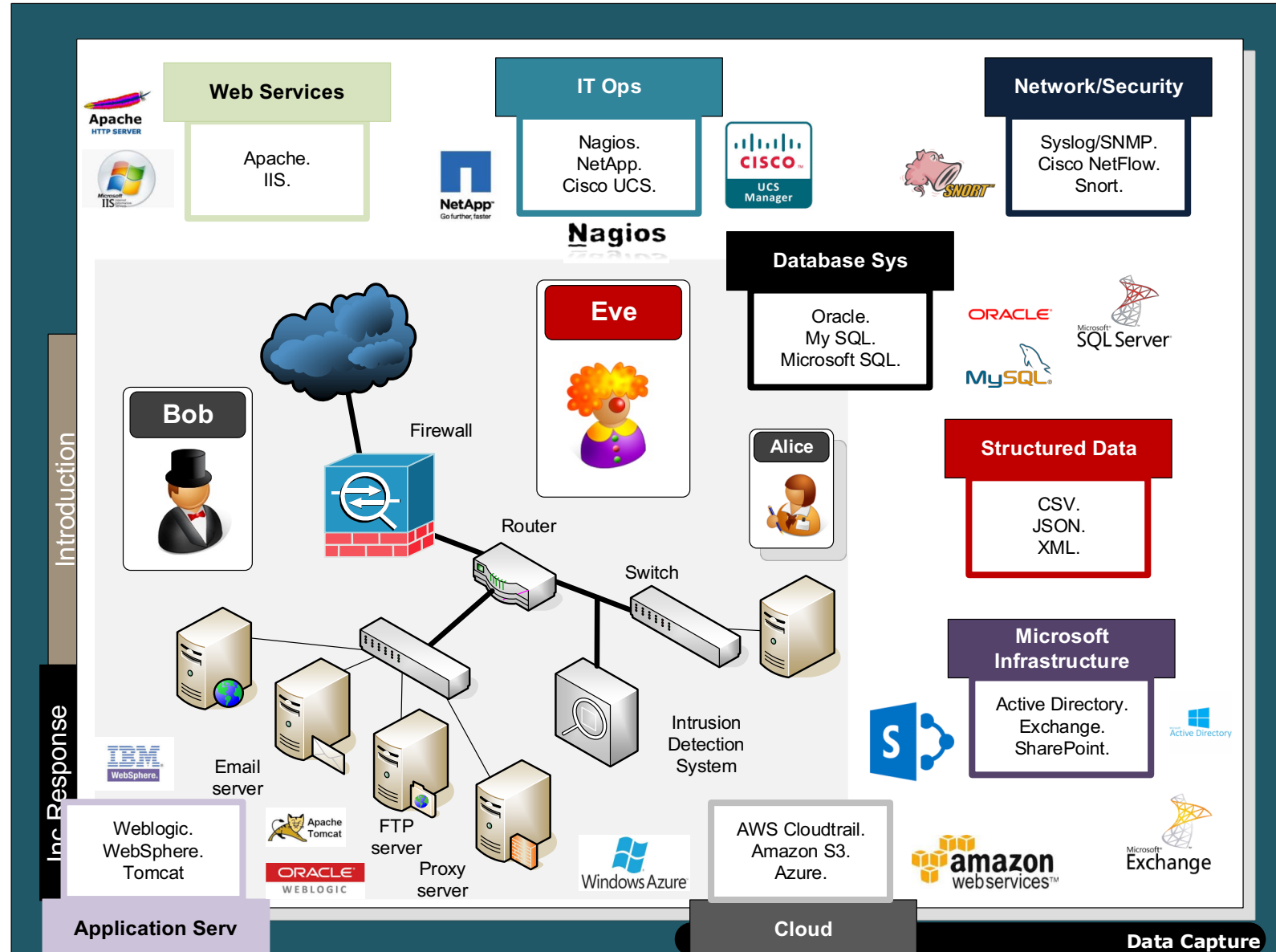
Data Analysis

- Increasing number of jobs are in Security Analytics (SOC Analysts).
- Companies require skills for before, during and after incidents (mix of security and forensics).



Increasing Complexity of Knowledge

- Increasing requirement for a wide range of skills for security professionals.

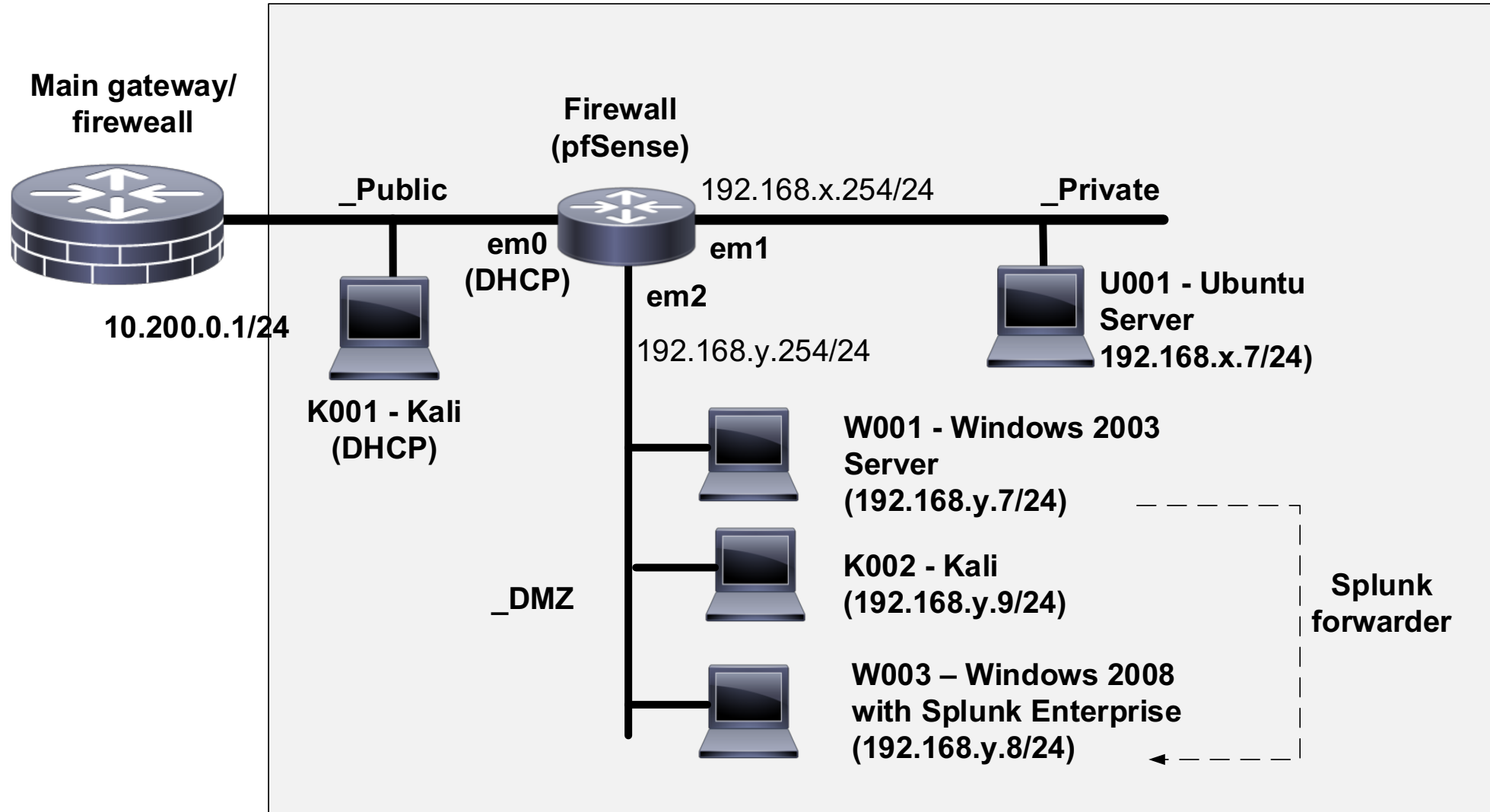




Design and Evaluation of [vSoC]: Virtualised Security Operations Centre

Splunk Lab Integration

vSoC SIEM Architecture



Splunk Lab Integration

The screenshot shows a desktop environment with a vSphere Client window in the background. The foreground features a web browser displaying a PDF document titled 'lab05_siem.pdf' from 'asecuritysite.com'. The document contains the following text:

network connection. In the lab you will be provided with network group in which you can select the LAN 192.168.x.0/24 and DMZ IP addresses 192.168.y.0/24 for configuration as shown in Figure 1.

The allocation of IP addresses is defined as Allocation A in:

<http://asecuritysite.com/csn11128/nets>

The diagram illustrates a network topology with the following components:

- Main gateway/firewall:** IP 10.200.0.1/24
- Firewall (pfSense):** Connected to the main gateway via interface `em0` and to the internal network via interface `em1`.
- Internal Network:** Divided into three segments:
 - _Public:** Contains `K001 - Kali (DHCP)`.
 - _Private:** Contains `W002 - Windows 7 (172.16.x.0/24)`, `U001 - Ubuntu Server (172.16.x.0/24)`, `W001 - Windows 2003 Server (172.16.y.7/24)`, `K002 - Kali (172.16.y.0/24)`, and `W003 - Windows 2008 with Splunk Enterprise (172.16.y.8/24)`.
 - _DMZ:** Contains `W003 - Windows 2008 with Splunk Enterprise (172.16.y.8/24)`.

A dashed box labeled 'Splunk forwarder' encompasses the `W003 - Windows 2008 with Splunk Enterprise (172.16.y.8/24)` node.

The desktop environment includes a taskbar with icons for Recycle Bin, FileZilla Server Interface, Mozilla Firefox, Opera, RdpGuard, Skype, VMware vSphere Client, and VMware vSphere... The system tray shows 'License Period: 57 days remaining' and 'SOCLAB:bbuchanan'.



Design and Evaluation of [vSoC]: Virtualised Security Operations Centre

Splunk Testing Environment –
Buttercupgames

SIEM

Back Click your answer, then NEXT and END when you are done to find out how you got on! [Download related content](#)

1 of 10 | [Prev.](#) [Next](#) [End](#)

<http://asecuritysite.com/tests/tests?sortBy=siem>

1. Refer to the Splunk analysis. For the access.log from www1, what is the top refer domain (Hint - source="d:\\buttercup\\www1\\access.log"| top limit=20 referer):

- A [www.bing.com](#)
- B [buttercupgames.com](#)
- C [google.com](#)
- D [www.yahoo.com](#)

New Search

buttercupgames

36,819 events (before 12/06/2016 14:54:17.000) No Event Sampling

Events (36,819) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

<http://asecuritysite.com:8000> 1 day per column

6,000 4,000 2,000

Sat Apr 19 2014 Mon Apr 21 Wed Apr 23 Fri Apr 25

List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 9 ... Next >

< Hide Fields All Fields

Selected Fields
a host 1
a source 3
a sourcetype 1

i	Time	Event
>	26/04/2014 17:22:16.000	91.205.189.15 - - [26/Apr/2014:18:22:16] "GET /oldlink?itemId=EST-14&SESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1665 "http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159 host = s18359064 ; source = D:\buttercup\www2\access.log ; sourcetype = access_combined_wcookie
>	26/04/2014 17:20:56.000	182.236.164.11 - - [26/Apr/2014:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&SESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko)



Capture The Flag

British Broadband, and RSA SA

British Broadband



How do hackers steal your ID?

9 November 2015 Last updated at 20:18 GMT

How difficult is it for cyber criminals to steal our identities?

Internet security expert James Lyne bought the stolen credit and debit card details of 13 people on the dark web as part of a



- Video: <https://www.youtube.com/watch?v=V7o03eLolqA>

British Broadband



British Broadband Details

Welcome to British broadband. We aim to provide you with the best current package detail includes fibre cables and coaxial, and we offer you the fastest service possible.

Current packages

Our Web packages are the best you can hope for and compare with you like our details, why not pass on the word, and tell our friends about our bill, and inform you of our new packages too.



News

We have been awarded the Britain's prize for most secure websites of 2016! Would you like to see everyone who contributed to the development of the most secure ISP in Britain!

To show you how thankful we are, we have decided to make it even easier for our users to access their records. Log in now to get started!

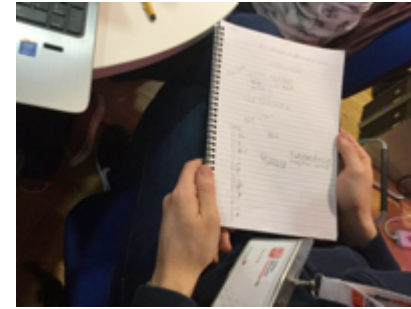
If you have forgotten your password, we also have implemented an easy way for you to generate a new one! I know it works, I've used it!

We are not afraid of so called "hackers" and we just proved it, once again!

Sincerely yours,
emily hambeef (CEO).

[reset password](#)

Cyber Security Insight Camp

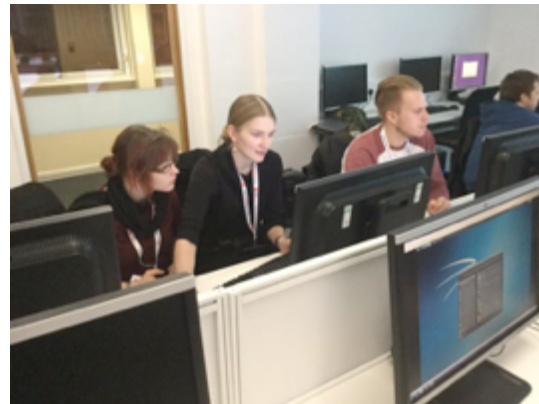


Cyber Security Insight Camp























5-7 March 2016

<http://thecyberacademy.org/cybercamp>






**CYBER
ACADEMY**

Scoreboard

#	Team	Country	Points
1	PatMikeClive		320
2	encryptthis		320
3	DojRoo		275
4	TheARMers		275
5	InsertNewTeamNameHere		270
6	NotChina		250
7	Mattam		245
8	HackingForGlory		220
9	CaribbeanKings		220
10	/tmp		195
11	whatever		175
12	doesntmatter		170
13	michaelmax		145
14	The Usual Suspects		120
15	TheNewKidOnTheBlock		95
16	abcd		50
17	Hopefuls		25
18	U2X2		25
19	IWILLDOMINATE		0
20	rewre		0

Heartbleed

This challenge has been solved by 63.2% of actively participating users.

Position	Team	Solved
1 	InsertNewTeamNameHere	1 day, 1 hour after release (2016-03-05 18:57:15)
2 	CaribbeanKings	1 day, 1 hour after release (2016-03-05 19:08:08)
3 	encryptthis	1 day, 1 hour after release (2016-03-05 19:12:46)
4	/tmp	1 day, 1 hour after release (2016-03-05 19:13:24)
5	doesntmatter	1 day, 1 hour after release (2016-03-05 19:14:26)
6	Mattam	1 day, 1 hour after release (2016-03-05 19:16:01)
7	HackingForGlory	1 day, 1 hour after release (2016-03-05 19:16:10)
8	PatMikeClive	1 day, 1 hour after release (2016-03-05 19:16:22)
9	TheARMers	1 day, 1 hour after release (2016-03-05 19:16:44)
10	michaelmax	1 day, 2 hours after release (2016-03-05 19:33:15)
11	DojRoo	1 day, 2 hours after release (2016-03-05 19:33:49)
12	NotChina	1 day, 2 hours after release (2016-03-05 19:36:29)

Pigpen (15pts)

⌚ 5 days, 23 hours, 39 minutes, 11 seconds remaining



Hint! <http://asecuritysite.com/content/pigpen.gif>

Please enter flag for challenge: Pigpen

Submit flag

Polybius (20pts)

⌚ 5 days, 23 hours, 39 minutes, 11 seconds remaining

15 32 15 13 45 43 24 13

Hint! <http://asecuritysite.com/content/poly.jpg>

Please enter flag for challenge: Polybius

Submit flag

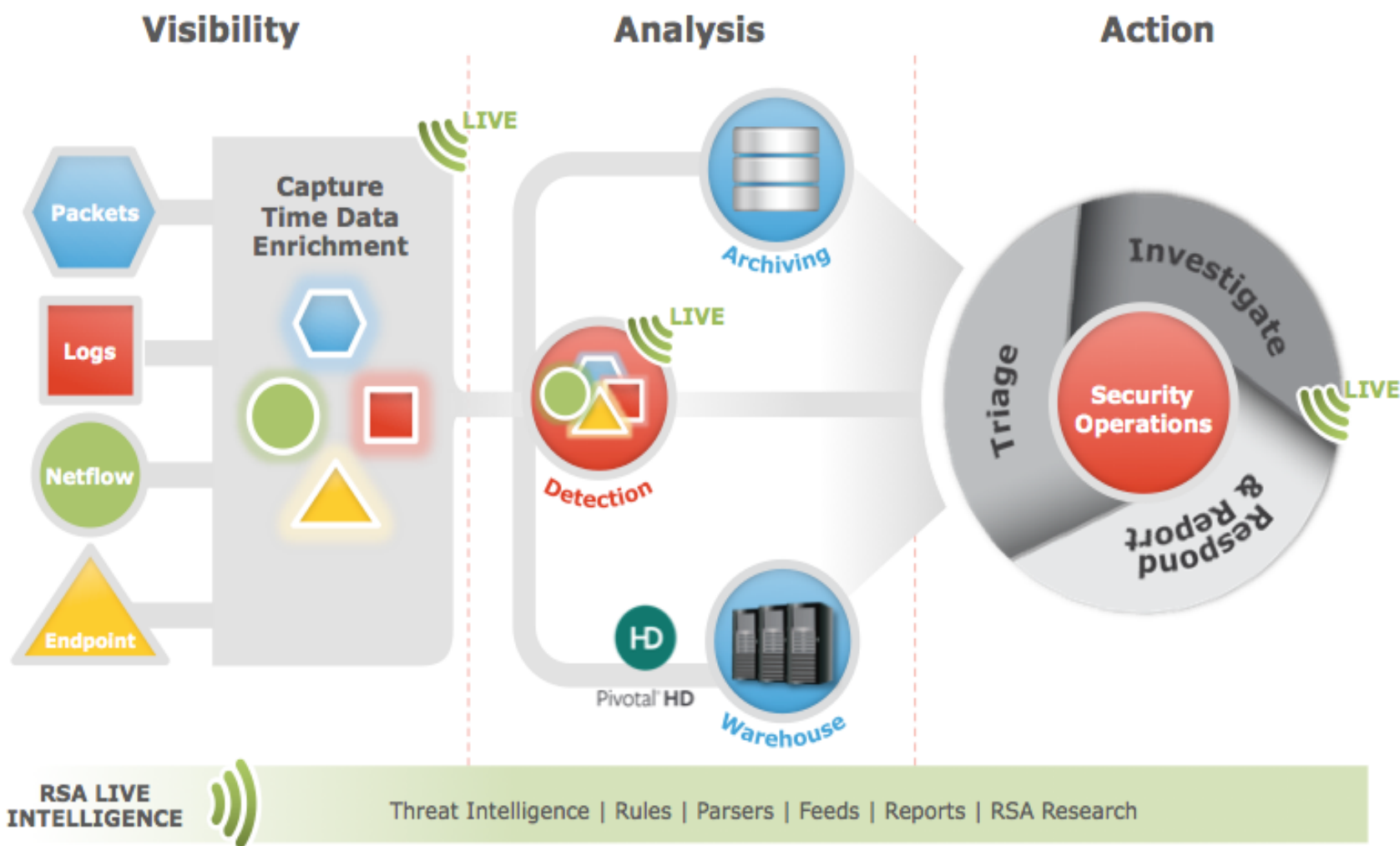
Ave Caesar (25pts)

⌚ 5 days, 23 hours, 39 minutes, 11 seconds remaining

Big Data in Cyber Security



RSA SA



CTF – Big Data in Cyber Security

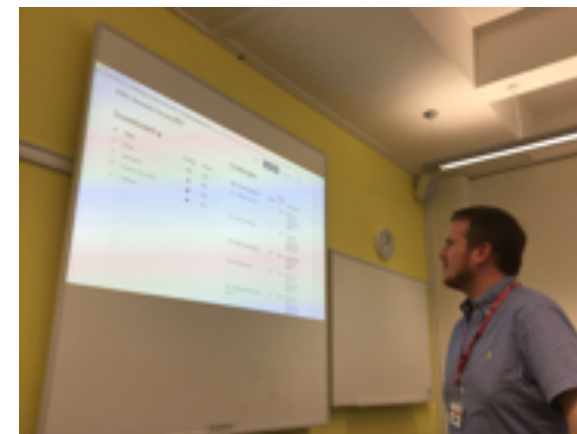
**CYBER
ACADEMY**

**International
Conference of Big
Data in Cyber
Security**



Partnership with HPE

theyberacademy.org



Security Analytics

**CYBER
ACADEMY**

Title	Description	Points	Visibility	Manage
Q1 - Timespan of events	When is the first and last event recorded Answ...	1		Edit Hint
Q2 - Events with emails	How many email addresses are highlighted in the tr...	5		Edit Hint
Q3 - Domain name request	Judging by DNS requests, which website has been vi...	10		Edit Hint
Q4 - 2013 traffic peak	For the 2013 activity, which day has the 2ND most ...	15		Edit Hint
Q5 - Most popular FTP user in 2013	Which FTP user has been logged in most often durin ...	20		Edit Hint
Q6 - Possible Spear phishing Attack	A spear phishing attack may have taken place. Whic ...	25		Edit Hint
Q6.1 - Victim of attack	The spear phishing attack was concerning a user at ...	25		Edit Hint
Q6.2 - Attacker	Which email address is the attacker using?	25		Edit Hint
Q6.3 - Attachment	What is the filename of the attacked file?	25		Edit Hint
Q6.4 - Phishing IP	What is the machine IP which received the spear ph ...	25		Edit Hint
Q6.5 - Data Exfiltration	What protocol has been used following the initial ...	25		Edit Hint
Q6.6 - Data Exfiltration contd.	What malicious user and passwords have been used t ...	25		Edit Hint
Q6.7 - Data Exfiltration contd.	What destination IP address has the data been sent ...	25		Edit Hint
Q6.8 - Data Exfiltration contd.	One of the extracted files share its name with a f ...	25		Edit Hint
Q7 - Web application data exfiltration attack	In the data an attacker is trying to exfiltrate pa ...	30		Edit Hint
Q8 - Telnet adventures	There is some suspicious Telnet network activity i ...	30		Edit Hint
Q8.1 - Going deeper	After the attacker gains access to the server, whi ...	30		Edit Hint
Q8.2 - Those 32 characters	Within the same session, were the attacker success ...	30		Edit Hint
Q8.3 - 32 char file obfuscated?	When was that file last modified? Type the answ ...	30		Edit Hint
Q8.4 - Another session	In the server subnet 192.168.5.0, can you identify ...	30		Edit Hint
Q8.5 - Sharing is caring	After the login, which directory is being connecte ...	30		Edit Hint

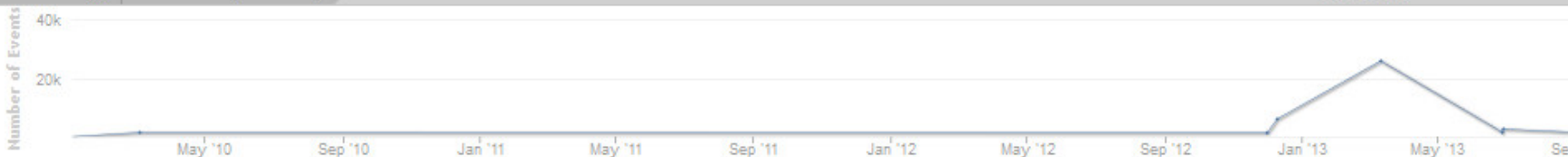
Navigate

Concentrator - Concentrator | All Data | Query | Profile | Meta | Total | Descending | Event Count | Save Events | Actions



2010 01 02 22:33:00 (+00:00)

All Data



Feed Description

Closed - Click to Open

Service Type (15 values)

HTTP (>1,000 - 5%) - OTHER (>1,000 - 6%) - DNS (>1,000 - 15%) - DHCP (>1,000 - 22%) - NETBIOS (>1,000 - 54%) - RPC (176) - SSL (163) - FTP (162) - SNMP (42) - SMTP (41) - TFTP (

Hostname Aliases (20 of 20+ values)

kali (1,471) - www.skylogistic.co.cc (362) - safebrowsing.cache.l.google.com (127) - bob-pc (107) - www.google.co.uk (106) - au.download.windowsupdate.com (101) - rsademo (!
- www.facebook.com (37) - pagead2.google syndication.com (35) - vip-lb.wordpress.com (34) - news.bbcimg.co.uk (31) - api.toptenreviews.com (31) - plus.l.google.com (28) - ss

Source IP Address (20 of 20+ values)

192.168.0.12 (18,995) - 172.16.0.16 (>1,000 - 8%) - 192.168.5.10 (5,397) - 192.168.0.3 (>1,000 - 27%) - 192.168.10.201 (3,302) - 0.0.0.0 (>1,000 - 31%) - 192.168.0.1 (>1,000 - 46%) - 192.
- 10.10.36.100 (293) - 192.168.75.144 (259) - 192.168.10.202 (248) - 192.168.10.50 (217) - 192.168.5.132 (126) - 192.168.0.14 (124) - 192.168.0.15 (118) ... show more

Destination IP address (20 of 20+ values)

192.168.0.4 (>1,000 - 10%) - 255.255.255.255 (>1,000 - 25%) - 192.168.0.3 (>1,000 - 27%) - 239.255.255.250 (>1,000 - 29%) - 192.168.0.13 (>1,000 - 37%) - 192.168.0.1 (>1,000 - 37%) - 1
- 192.168.75.132 (1,123) - 192.168.0.7 (1,081) - 192.168.0.10 (990) - 192.168.5.172 (969) - 192.168.10.255 (791) - 172.16.0.254 (761) - 192.168.5.169 (703) - 192.168.5.145 (613) - 192.1

Source IPv6 Address (19 values)

fe80:0:0:4d29:6d58:6e01:6327 (254) - fe80:0:0:0:d013:692d:9526:6d12 (47) - 0:0:0:0:0:0:0:0 (16) - fe80:0:0:0:19c9:691:2da8:ba2 (15) - fe80:0:0:0:8d78:36bd:bfd8:19f0 (8) - fe80:0:0:0:
- fe80:0:0:0:250:56ff:feab:6d53 (3) - fe80:0:0:0:6ddd:73f9:ad56:512c (2) - fe80:0:0:0:1880:c13a:ad39:eb30 (2) - fe80:0:0:0:a00:27ff:fefe:8f95 (2) - fe80:0:0:0:4e17:ebff:fe64:1649 (1) - fe
- fe80:0:0:0:20c:29ff:fe83:3fed (1)

Destination IPv6 address (16 values)

ff02:0:0:0:0:0:1:3 (171) - ff02:0:0:0:0:0:1:2 (81) - ff02:0:0:0:0:0:c (69) - ff02:0:0:0:0:0:2 (13) - ff02:0:0:0:0:1:ff01:6327 (8) - ff02:0:0:0:0:0:fb (6) - ff02:0:0:0:0:0:16 (6) - ff02:0:0:0:0:0:1
- fe80:0:0:0:a00:27ff:fefe:8f95 (1) - fe80:0:0:0:a00:27ff:fed4:10bb (1) - ff02:0:0:0:1:ffe:8f95 (1) - ff02:0:0:0:1:ff83:3fed (1)



Design and Evaluation of [vSoC]: Virtualised Security Operations Centre

Results

Current Range of VMs

- Specialised: EnCase, Windows XP (with Malware), GNS3.
- Linux Kali.
- Ubuntu.
- Windows 2003, Windows 2008, Windows 7 and Windows 8.
- Firewalls: pfSense, vyatta, F5 Big-IP (in development).
- Caine.
- Metasploitable.

Example

Create VM

Setup network

Create known
snapshot

```
$tubuntu = "t_ubuntu_205"

if ($args[1].contains("u"))
{
    $ins = $prefix+$iubuntu +$i.ToString("000")+ "_private";
    ...
    Write-Output "Creating: $($ins) from $($temp) in $($folder) for $($folder) disk:
    $($disk) "
    new-vm -name $ins -template $temp -datastore $disk -resourcepool DFETLab -
    DiskStorageFormat thin -location $folder

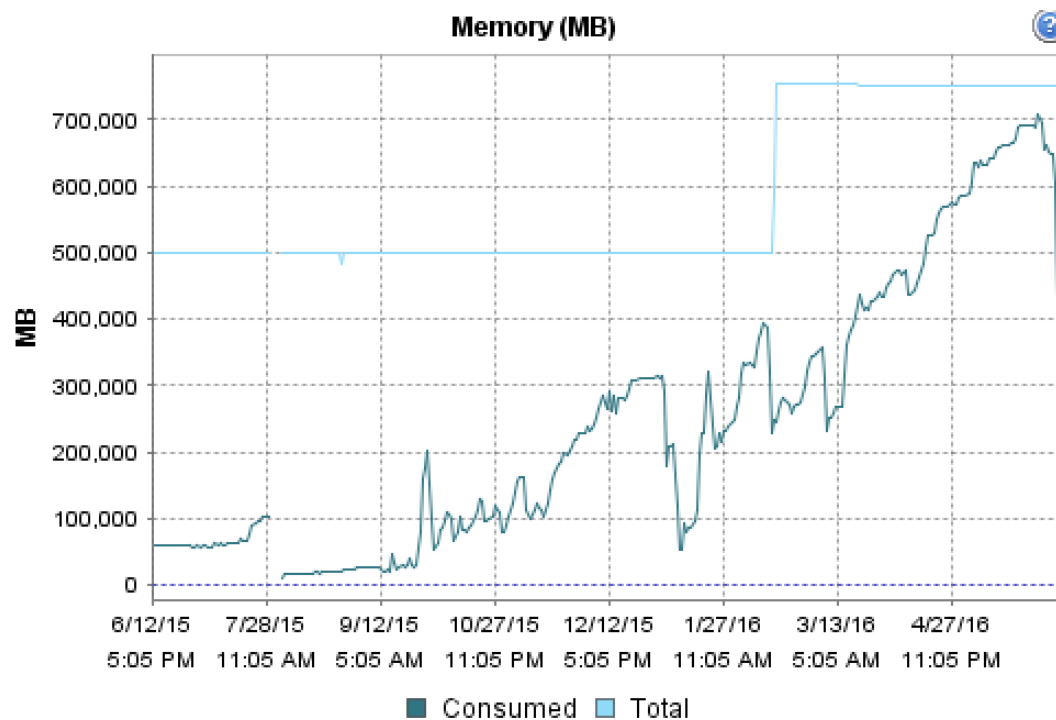
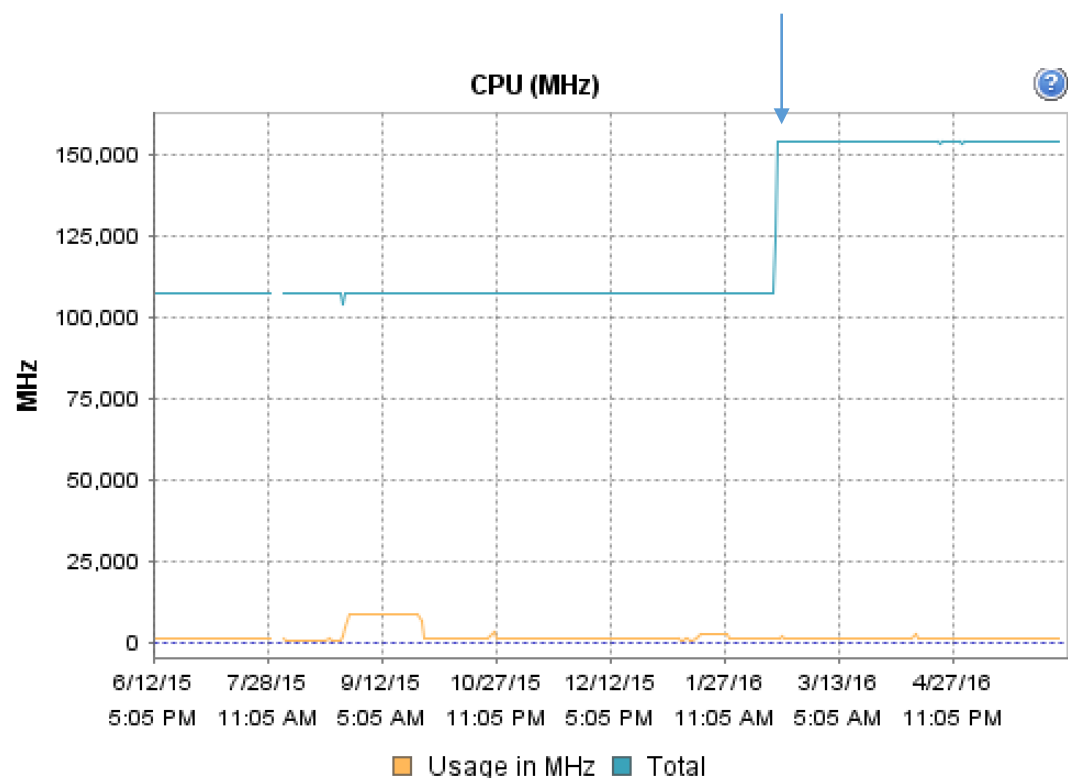
    $apt = Get-NetworkAdapter -VM $ins
    Set-NetworkAdapter -NetworkAdapter $apt -NetworkName $private -
    confirm:$false

    Write-Output "Creating: $($ins) from $($temp) in $($folder) for $($folder) disk:
    $($disk) "

    new-snapshot -VM $ins -Name snapshot
}
}
```

Results

Cloud upgrade



Modules used on:

Semester 1: Cryptography and Network Forensics (80 students); Network Security (60 students – GNS3); Host-based Forensics (60 students - EnCase).

Semester 2: Security Testing (70 students); e-Security (100 students); Incident Response and Malware Analysis (100 students).



ArcSight  RSA SECURITY ANALYTICS

 splunk 



SDN Integration

Prof William J Buchanan, Charley Celice, Peter Aaby, Bruce Ramsay, Richard Macfarlane, Adrian Smales, Dr Gordon Russell and Bobby Soutar

<http://thecyberacademy.org>

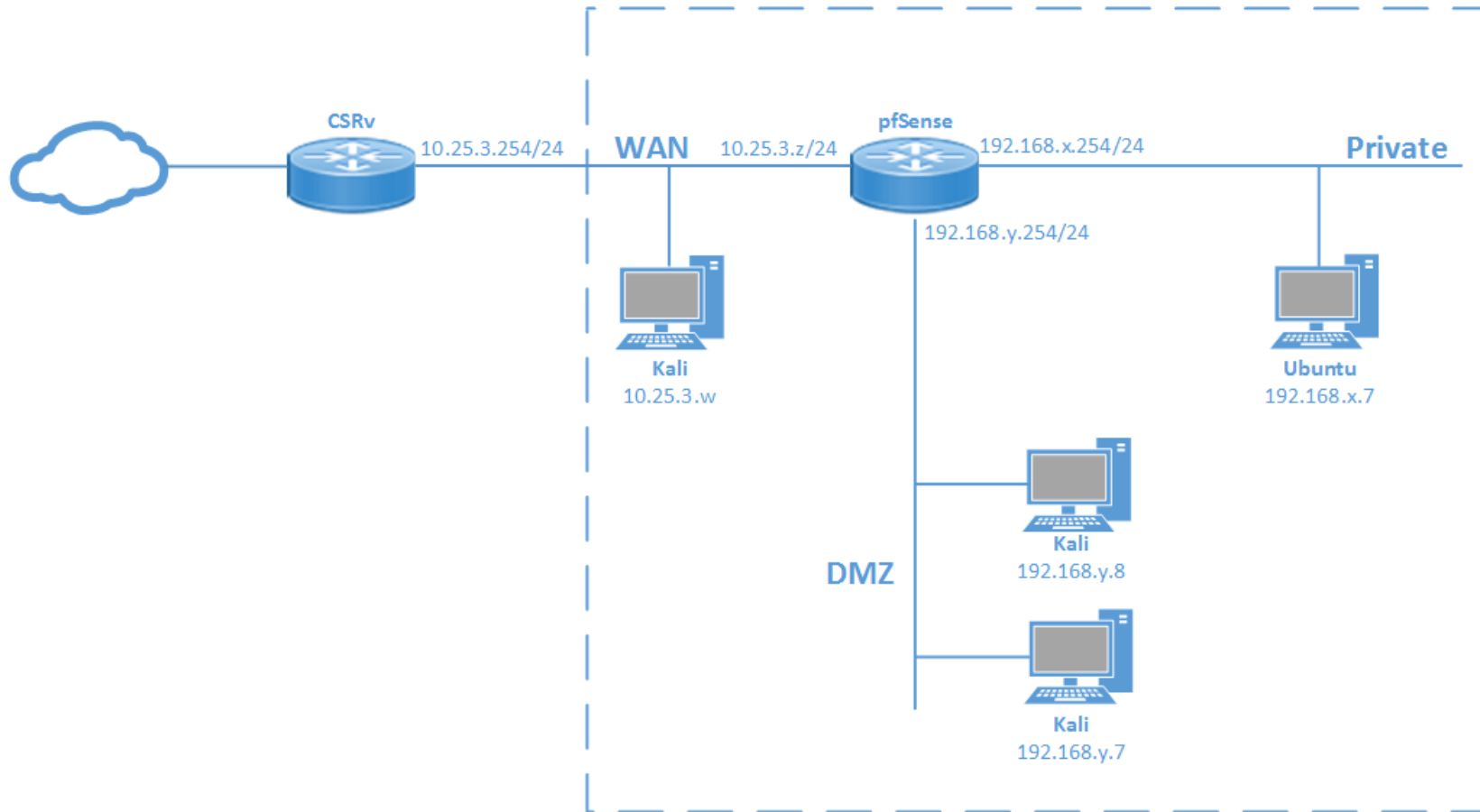
Current Work

- Integrating F5 Big-IP (30 licences).
- Integration of SDN within Cloud (with Hutchinson Networks).
- Integration of RSA SA and Splunk for teaching in 2016/2017.
- Integration of HPE Arcsight.
- Roll-out of two CTF: British Broadband and RSA SA (Network Forensics).
- Development of a mobile Cloud environment, for onsite training/CTF.



Current Work

Lab Infrastructure



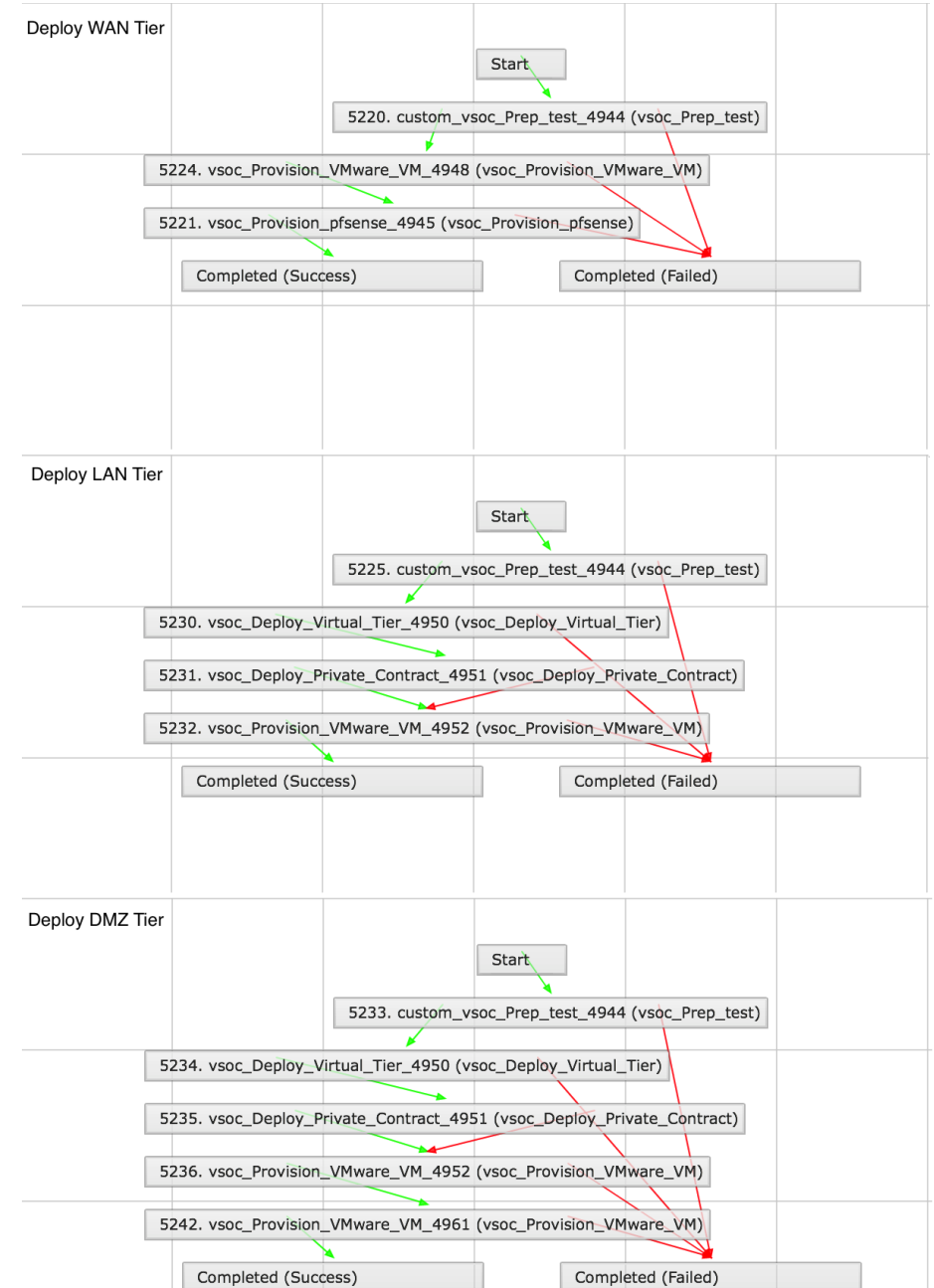
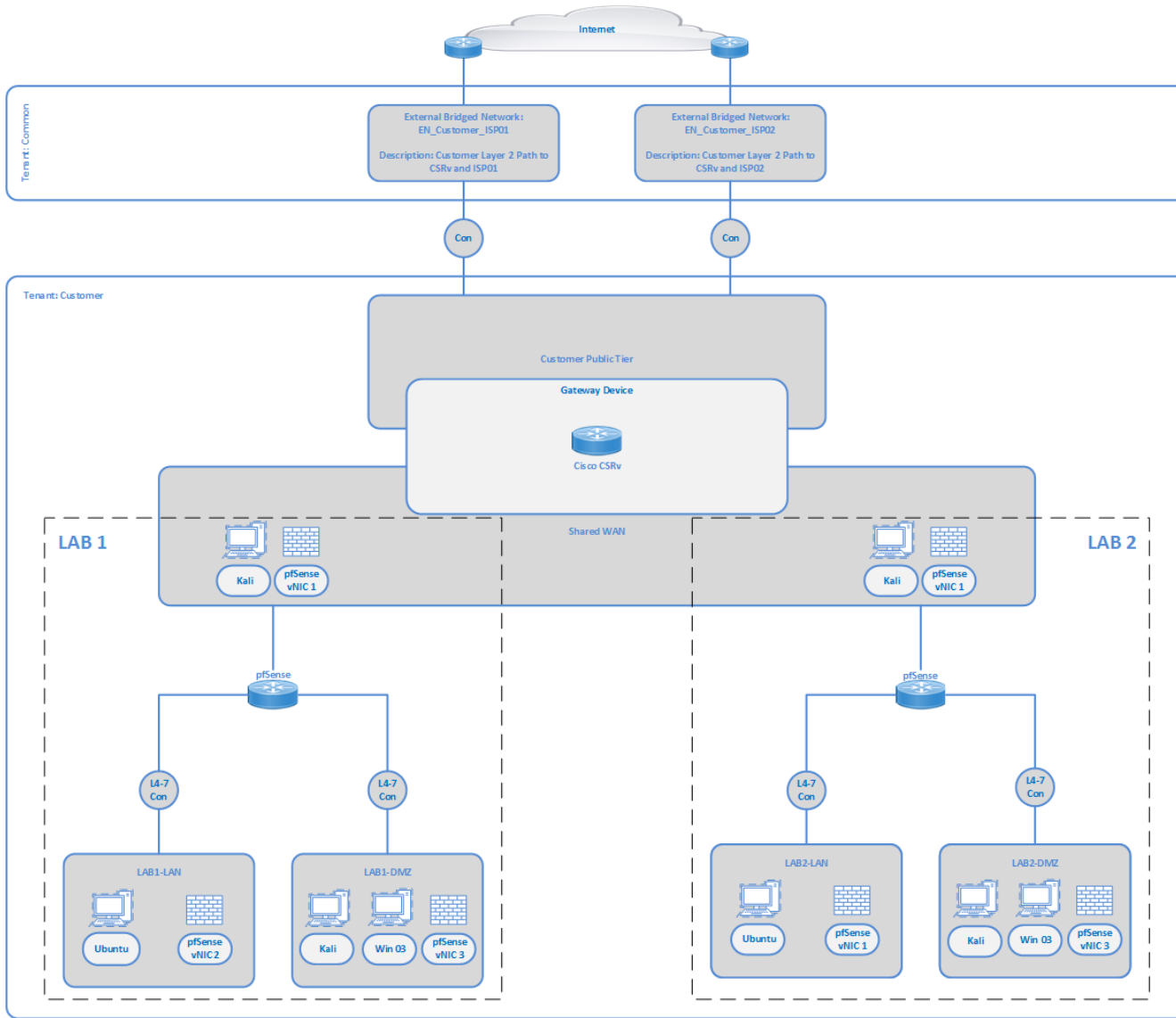
fabrix

RSA Security Analytics

ArcSight
An HP Company

**CYBER
ACADEMY**

Current Work



CS



Current Work

fabrix YOUR FABRIX

Dashboard myfabrix

Catalog Services Virtual Resources Accounting

Catalog

Refresh

Catalog

VM Deployment Networking

Total 33 items

fabrix YOUR FABRIX PROFILE PRICING HELP LOG OUT

Dashboard myfabrix

Catalog Services Virtual Resources Accounting

Catalog

Refresh

Catalog

Top > Napier vSOC

Windows 2003 LND01VMDC01

KALI LND01VMDC01

Ubuntu LND01VMDC01

Metasploitable LND01VMDC01

Windows XP LND01VMDC01

Windows 7 LND01VMDC01

Deploy Architecture

Deploy Additional Labs

Delete VMs

fabrix YOUR FABRIX PROFILE PRICING HELP LOG OUT

Dashboard myfabrix

Catalog Services Virtual Resources Accounting

Virtual Resources

Summary vDCs Application Containers VMs VM Action Requests Images Port Groups DV Port Groups Resource Pools More Reports

Refresh View Details Access VM Credentials Launch VM Client Resize VM Power ON Power OFF Delete VM Suspend Shutdown Guest Reset Reboot

lab1

Cloud	Request ID	VM-ID	VM Label	VM Name	Host Name	IP Address	Power State	vDC	Category	Provisioned Time	Scheduled Time	Guest OS Type
LND01VMDC01	44422	1313	Kali-DMZ	Lab1-Kali-DMZ-44422	kali		OFF	LND01VMDC01_	Generic VM	06/09/2016 11:3		Other 2.6.x L
LND01VMDC01	44337	1296	Kali-PUB	Lab1-Kali-WAN-44337	kali		OFF	LND01VMDC01_	Generic VM	06/09/2016 10:4		Other 2.6.x L
LND01VMDC01	44420	1308	Ubuntu-LAN	Lab1-Ubuntu-Priv-44420	ubuntu		OFF	LND01VMDC01_	Generic VM	06/09/2016 11:3		Ubuntu Linux
LND01VMDC01	44460	1317	Win03-DMZ	Lab1-W03-44460			OFF	LND01VMDC01_	Generic VM	06/09/2016 12:0		Microsoft Win
LND01VMDC01	44378	1302	pfSense	Lab1-pfsense-44378			OFF	LND01VMDC01_	Generic VM	06/09/2016 11:1		Ubuntu Linux



Current Work



fabrix

Security Analytics

ArcSight
An HP Company

**CYBER
ACADEMY**



ArcSight  RSA SECURITY ANALYTICS

 splunk 



Design and Evaluation of [vSoC]: Virtualised Security Operations Centre

Prof William J Buchanan, Charley Celice, Peter Aaby, Bruce Ramsay, Richard Macfarlane, Adrian Smales, Dr Gordon Russell and Bobby Soutar

<http://thecyberacademy.org>