

BT CERT Training Cell

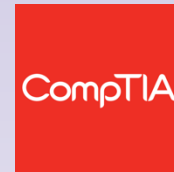


Practical Forensic Readiness in Security Operations



Introductions

- Clem Craven
- Matt Scott
- Ian Wilson





1000
customers



170 countries

108+ registered patents
and **190+** security papers



**We protect BT
and its customers**



We monitor
40,000+
devices



2500 security practitioners

14

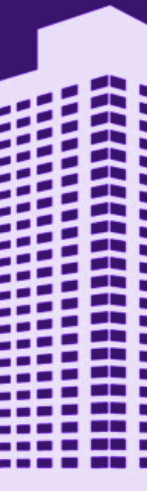
follow-the-sun
SOCs



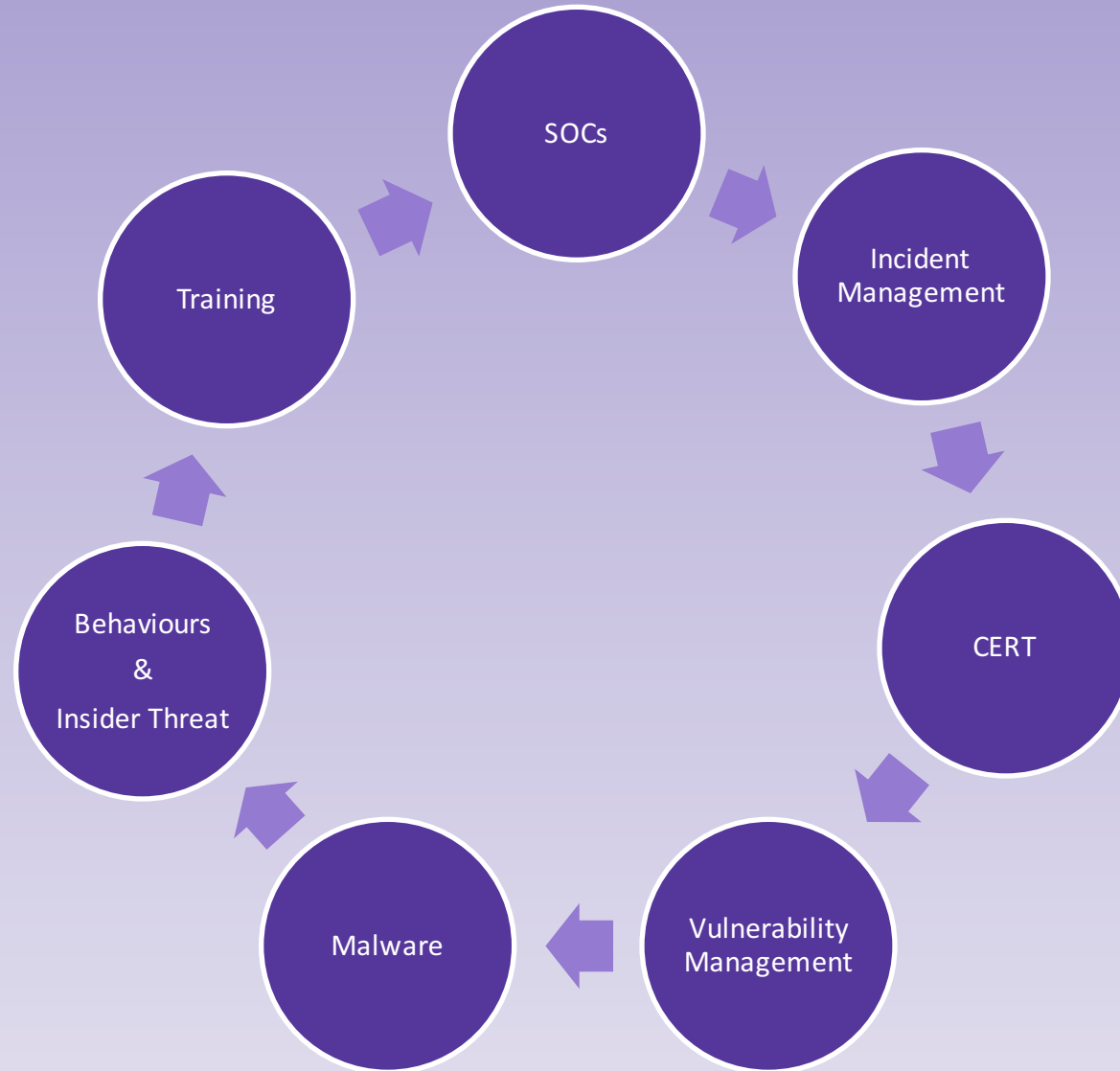
Our cyber defence operations unit

provides insight ahead of and
during security incidents

We protected the **London 2012**
Olympic and Paralympic Games



Introductions - BTCERT



Objectives

- To improve awareness of forensic readiness in security operations.
- To describe methods used to make forensic readiness capabilities more efficient.



What is forensic readiness?

“Forensic Readiness is the achievement of an appropriate level of capability by an organisation in order for it to be able to collect, preserve, protect and analyse digital evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal, UK Court of law or Parliamentary enquiry.”

(UK - CESG Good Practice Guide 18 – Forensic Readiness)

Translation: During an investigation you need to ensure;

- Your investigation holds up to scrutiny.
- It promotes impartiality and transparency.
- You don't miss anything.



How to do forensic readiness?



Start early



Note Taking



Chain of
Custody



Peer Review



Post
incident
review



Starting Early – Policy

- Forensic Policy
- Business Ownership
- SPOC
- Definition of Capability and Requirements
- Quality Assurance and Competence
- Legal Disclosure
- Investigation Standards (ACPO)/Protective Monitoring



ACPO - UK



Principle 1

No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.



ACPO - UK



Principle 2

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.



ACPO - UK



Principle 3

An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.



ACPO - UK



Principle 4

The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.



What is evidence?

Evidence is used to indicate the means by which any fact or point in issue or question may be proved or disproved in a manner complying with the legal rules governing the subject.

Translation:

- Something which can prove something has happened or hasn't happened.
- It can be anything.
- Dependent on local laws or organisational policies.



Types of evidence

- Real Evidence
- Documentary Evidence

- ‘Real evidence consists of the production of material objects for the inspection by the judge and jury, or magistrates in court’.



Types of evidence

- Real Evidence
- Documentary Evidence

- This encompasses anything which communicates a visual image to a human being.



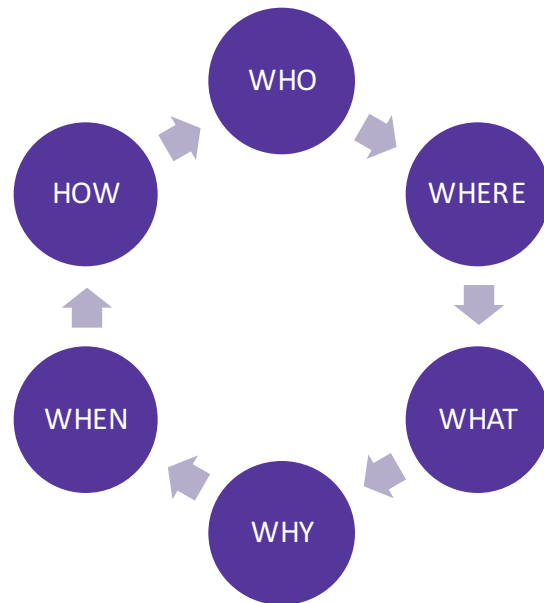
Starting Early – Investigations

- Go Bags
- Contracts written in a forensically sound fashion
- Third Party supply chains and outsourcing
- Appreciation of cost
- Scaling of forensic readiness
- Mandated training



Note Taking

- Document your actions



- Do it yourself?
- Do it with a buddy?



Note Taking

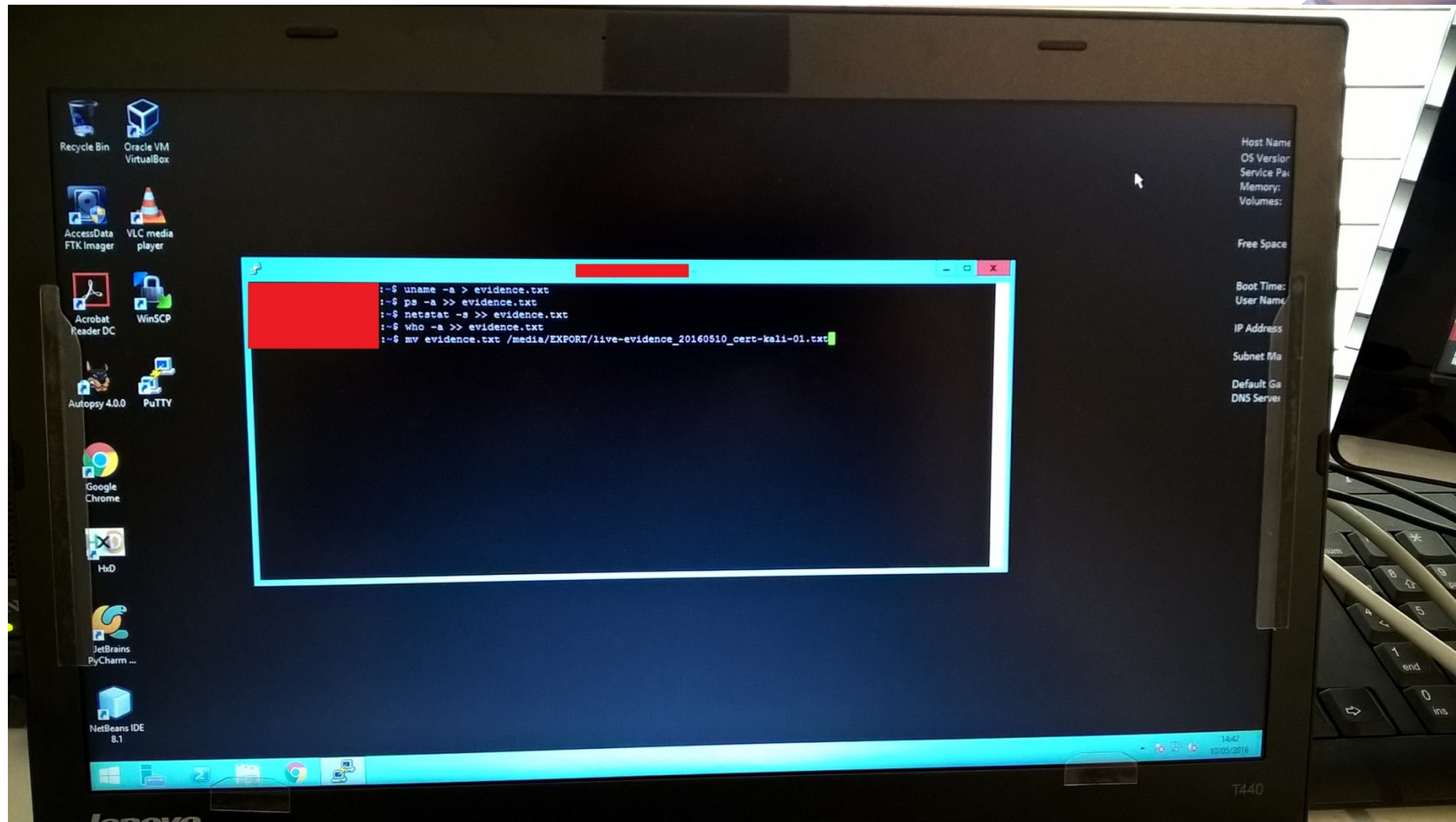
- Copy commands entered and output
 - Screenshots
 - Photographs
 - Video
 - Shell history



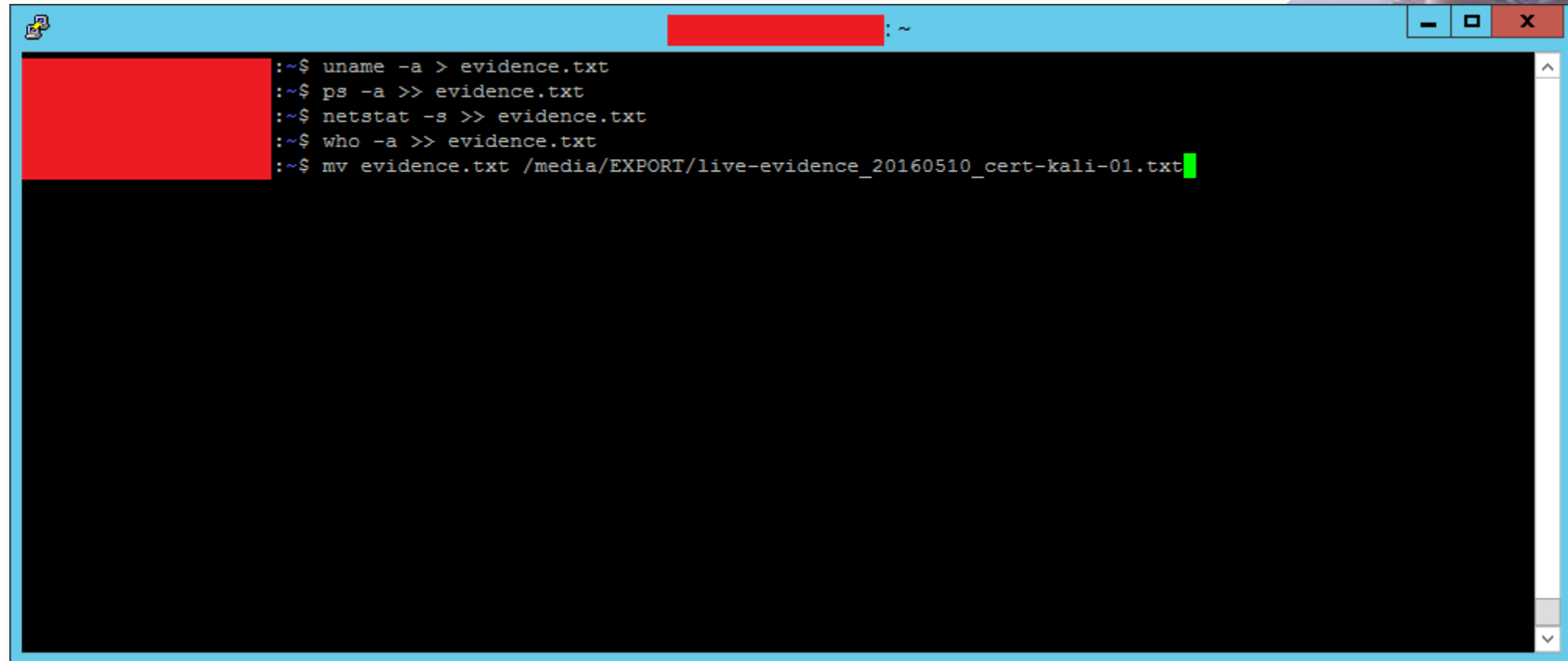
Note Taking



Note Taking



Note Taking

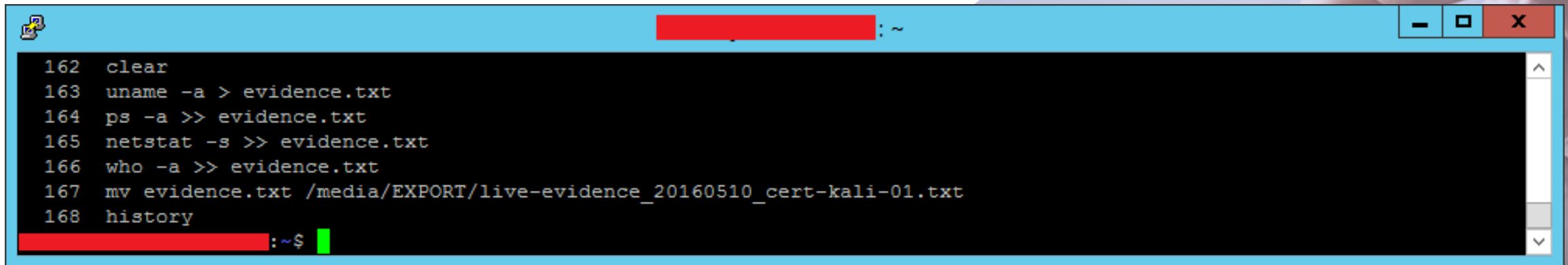


A terminal window with a blue title bar and a black background. The window title is partially obscured by a red box. The terminal shows a series of commands being executed to collect system information and save it to a file named 'evidence.txt'. The commands are: 'uname -a > evidence.txt', 'ps -a >> evidence.txt', 'netstat -s >> evidence.txt', 'who -a >> evidence.txt', and 'mv evidence.txt /media/EXPORT/live-evidence_20160510_cert-kali-01.txt'. A green cursor is visible at the end of the last command.

```
~$ uname -a > evidence.txt
~$ ps -a >> evidence.txt
~$ netstat -s >> evidence.txt
~$ who -a >> evidence.txt
~$ mv evidence.txt /media/EXPORT/live-evidence_20160510_cert-kali-01.txt
```



Note Taking



```
162 clear
163 uname -a > evidence.txt
164 ps -a >> evidence.txt
165 netstat -s >> evidence.txt
166 who -a >> evidence.txt
167 mv evidence.txt /media/EXPORT/live-evidence_20160510_cert-kali-01.txt
168 history
```

The image shows a terminal window with a blue title bar. The window title is partially obscured by a red bar. The terminal content shows a series of commands numbered 162 to 168. The prompt is a red bar followed by a green cursor. The background of the slide features a woman looking at a laptop.



Note Taking

- Templates and checklists
 - Prompt to perform certain actions
 - Link to processes recording how you did it
 - Prompt to record when complete



Note Taking

Email Fields		
Email Subject	:	
Email To	:	
Email From	:	
Email Date/Time	:	
Email Attachment(s)?	:	No
Email Link(s)?	:	No
Email Description	:	

Net Traffic Fields		
Traffic Time	:	24/08/2015 12:51:09
Traffic Source IP & Port	:	[REDACTED] : [49464]
Traffic Protocol	:	TCP
Traffic Dst IP & Port	:	[REDACTED] : [80]
Traffic Description	:	
GET/POST URL	:	



Note Taking

CERT INVESTIGATION TEMP... ▾

Intro OVERVIEW ACTIONS IDENTIFICATION CONTAINMENT ERADICATION RECOVERY DOCUMENTS EMAILs CLOSURE RFCs +

IDENTIFICATION

Is this an Incident or just some random deviation from the norm (e.g. failing hardware)?

Given the nature of the reported incident what steps have been taken, by whom, when, where, how and why in order to establish a fuller picture and establish if this is an incident.

E.g. For Code Red we used Splunk to examine the log file

Perhaps use this space to record the name of the log file, the splunk query used and a screen cap or export to show the results with the Team member giving a précis. This would confirm an incident has taken place.

POINTS TO REMEMBER:

- Where did the incident occur?
- Who reported or discovered the incident?
- How was it discovered?
- Are there any other areas that have been compromised by the incident? If so what are they and when were they discovered?
- What is the scope of the impact?
- What is the business impact?
- Have the source(s) of the incident been located? If so, where, when, and what are they?

DATE	WHO	ACTION



Note Taking

- Incident coordination – identify and manage your tasks
 - List tasks
 - Assign to individuals
 - Track task completion



Note Taking

Tasks

<input type="checkbox"/>	ID	Title	<input type="checkbox"/> Assigned To	Status	Start Date	Due Date	Priority	Modified	<input type="checkbox"/> Modified By
	11	Analyse disk image <small>NEW</small>	Wilson, I, Ian, VQH1 R	Not Started	18/05/2016	20/05/2016	(2) Normal	18/05/2016 01:38 PM	Scott, MJ, Matthew, VQH1 R
	10	Isolate host and collect disk image <small>NEW</small>	Scott, MJ, Matthew, VQH1 R	In Progress	18/05/2016	18/05/2016	(2) Normal	18/05/2016 01:36 PM	Scott, MJ, Matthew, VQH1 R

[+ Add New Task To Incident](#)



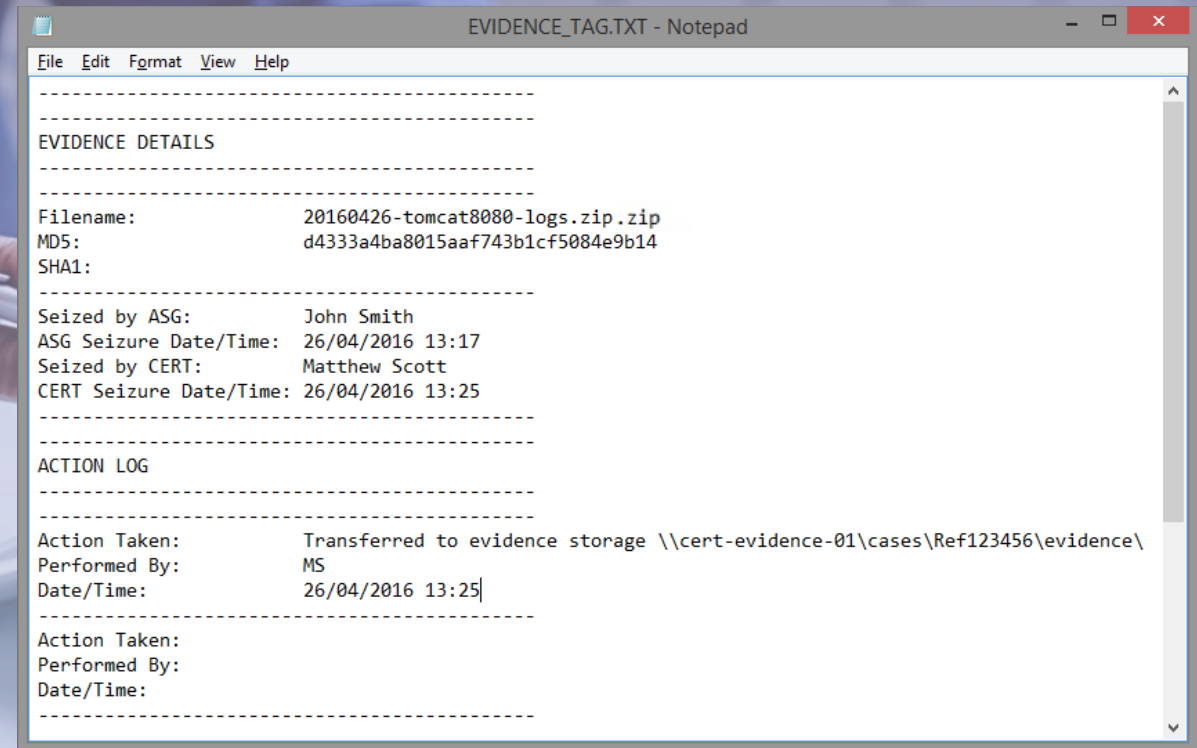
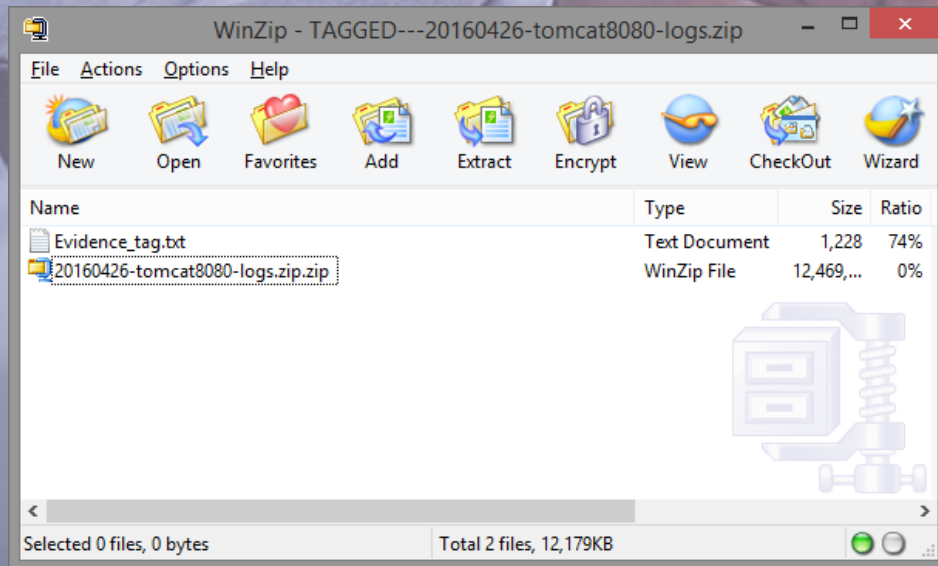
Chain of Custody

- Maintain evidence integrity
 - Collection and storage
 - Record in notes
 - Auditable



Chain of Custody

- Digital “bag and tag”
 - Text file (tag) and evidence file in zip archive (bag)



Chain of Custody

No. ↓	Modified	Modified By
6.0	15/03/2016 13:24	Instructor01
	Event Title 1636 - Clem WT Demostation - Code Red	
5.0	15/03/2016 13:24	Instructor01
	Event Status Send for Closure Approval	
	Cause This was a firing f Code red across the network	
	Resolution lma;ljkldslklklkj	
	Closing Comments More education is needed for the users and make sure that the least privilege	
	Event Title - Clem WT Demostation - Code Red	
4.0	14/03/2016 13:41	Instructor01
	Event Title 1636 - Clem WT Demostation - Code Red	
	MSREPORT DATE 24/02/2015 15:00	
3.0	14/03/2016 13:41	Instructor01
	Cause	
	Resolution	
	Closing Comments	
	Bottom Line Up Front (BLUF) A Code red attack on the system with the IP addresses listed as being involved.	
	Owned By IRDM DAYS	
	Closure Review	
2.0	14/03/2016 13:37	Instructor01
1.0	14/03/2016 13:37	Instructor01
	Title Clem WT Demostation - Code Red	
	Comments Whilst looking a the SIEM, there was an alert which came from 25.16.13.9 and this attacked a few hosts.	
	Method of Detection --Please Select--	
	Event Ref - Clem WT Demostation - Code Red	
	Blackthorn Ref 1001	
	Classification RES	
	Event Location North Star House, North Star Avenue Swindon SN2 1BS	
	Sensor Snort:25 xx xx xx xx	
	Event Status Open	
	Related to Incident Unrelated to any Incident as of yet.	
	Initial Priority 3.6	
	Current Priority 3.6	
	Event Category Virus / Trojan	
	Methods of Detection IDS	



Peer Review

- Quality Assurance
 - Perform an action, colleague checks action
 - Reduces human error
 - Responsible decision making



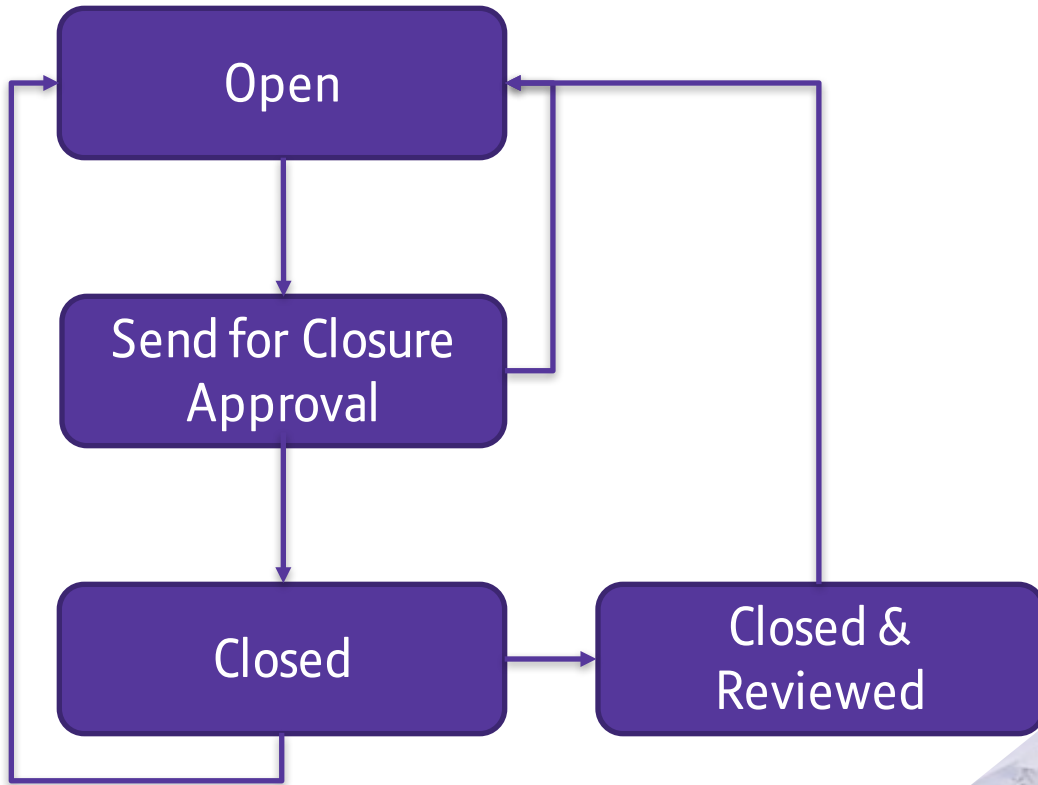
Peer Review

Edit Event: 20150127 - Compromise - UDP

Title *	<input type="text" value="20150127 - Compromise - UDP"/>
False Positive	<input type="checkbox"/> The underlying signature did not fire on the content that it was supposed to.
Missing Packets	<input type="checkbox"/> If this is ticked, there must be corresponding Incident Note(s) explaining the missing packets.
Other Ref	<input type="text" value="RAFP/Sy/01"/>
Event Status ?	<input type="text" value="Send for Closure Approval"/>
Descriptive Event Category *	<input type="text" value="Send for Closure Approval"/> orisatio



Peer Review



Current User Current Case Status	Analyst (Permissions Available)	Shift Leader (Permissions Available)	Reviewer (Permissions Available)
Open	Open Send for closure approval	Open Send for closure approval	Open Send for closure approval
Send for Closure Approval	Send for closure approval	Open Send for closure approval	Send for closure approval
Closed	Closed	Open Closed	Close Closed & Reviewed
Closed & Reviewed	Closed & Reviewed	Open Closed	Closed & Reviewed



Post Incident Review

- Write an incident report
 - Capture actions and lessons
 - Presentable and accessible
 - Trustworthy threat intelligence



Post Incident Review

1.0 Incident Ref (Insert ticket reference if applicable)	1.1 Date Incident Opened (date of occurrence)	1.2 Date Incident Closed (date of closure)	1.3 PIR Status (closed / in-progress etc.)
xxxxxxx	dd/mm/yy	dd/mm/yy	xxxxxx
2.0 Incident Summary (Insert high level summary of incident)			
3.0 Impact (Insert recorded business impact)			
4.0 Communications (What communications have been sent)			
5.0 Process (What Process & Playbook have been used and has it been circumvented)			
6.0 Timeline of events			
ID	Date / Timestamp	Event	
7.0 Root Cause (Insert recorded root cause if known)			
8.0 Risk Mitigation (Were any actions taken to mitigate the impact on the business / service?)			
9.0 Prevention of Reoccurrence (What is the current risk to service / business of reoccurrence? What actions need to be completed to reduce this?)			
10.0 Recommendations / Lessons Learned (Any recommendations or lessons learned for future PIRs)			
<i>Important Note: Any recommendations made should be prioritised according to their potential risk to the business for 'non completion' and 'cost of completion' (if known):</i>			
11.0 Comments (Anything worthy of note)			



Post Incident Review

IP ADDRESS

This is an "Address" [CyBox](#) object.

193.124.185.87
217.12.199.94
185.82.202.170
37.46.131.153
92.222.71.26

DOMAIN NAME

This is a "Domain Name" [CyBox](#) object.

[ouybncuataejqatde.xyz](#)
[huabpsbuure.work](#)
dpeltqlxummpwfj.info
ofbcwtfdkhxlivjm.pw
[stwmkvi.click](#)
chfalxeuphlatvj.su
pwxsfbytiyskllw.info
jltjkkobdfp.pw
nrfdxkingkxy.su
qbaakkiqhof.su
effacip.org
gkiwgtaufpyv.org

FILE ([Cybox File](#))

This is a "File" [CyBox](#) object.

OTHER

State the IOC and the corresponding [CyBox](#) object.

IOC	CyBox Object
/userinfo.php	Link



What do you get out of forensic readiness?

- More efficient and more impactful intervention
 - Criminal court
 - Civil court
 - Parliamentary Enquiry / Congressional Hearings
 - Employee tribunal
 - Industry collaboration
- Evidence-based decision making
- Create better threat intelligence
- Use better threat intelligence



Outcomes

- ✓ To improve awareness of forensic readiness in security operations.
- ✓ To describe methods to make forensic readiness capabilities more efficient.
- ✓ Reduce evidential errors.
- ✓ Increase success.
- ✓ Be efficient.



References

- Association of Chief of Police Officers – Good Practice Guide for Computer-based Electronic Evidence.
 - [https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence\[1\].pdf](https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].pdf)
- CESG – Good Practice Guide 18 Forensic Readiness
 - [https://www.cesg.gov.uk/content/files/guidance_files/Forensic%20Readiness%20\(Good%20Practice%20Guide%2018\)_1_2.pdf](https://www.cesg.gov.uk/content/files/guidance_files/Forensic%20Readiness%20(Good%20Practice%20Guide%2018)_1_2.pdf)
- CESG – Good Practice Guide 13 Protective Monitoring
 - https://www.cesg.gov.uk/content/files/guidance_files/Protective%20Monitoring%20for%20HMG%20ICT%20Systems%20%28Good%20Practice%20Guide%2013%29_1.7.pdf





Questions & Discussion





BT CERT Training Cell.
Security Through Knowledge.

