BT CERT Training Cell

Practical Forensic Readiness in Security Operations
Introductions

- Clem Craven
- Matt Scott
- Ian Wilson
1000 customers

108+ registered patents and 190+ security papers

170 countries

20 partners and over 200 security vendors

14 follow-the-sun SOC's

2500 security practitioners

We monitor 40,000+ devices

We protect BT and its customers

Our cyber defence operations unit provides insight ahead of and during security incidents

We protected the London 2012 Olympic and Paralympic Games
Introductions – BTCERT

- Training
- Behaviours & Insider Threat
- Malware
- CERT
- SOC
- Incident Management
- Vulnerability Management
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
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.
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.
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.
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

```bash
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
```
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

<table>
<thead>
<tr>
<th>Email Fields</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Subject</td>
<td>:</td>
</tr>
<tr>
<td>Email To</td>
<td>:</td>
</tr>
<tr>
<td>Email From</td>
<td>:</td>
</tr>
<tr>
<td>Email Date/Time</td>
<td>:</td>
</tr>
<tr>
<td>Email Attachment(s)?</td>
<td>No</td>
</tr>
<tr>
<td>Email Link(s)?</td>
<td>No</td>
</tr>
<tr>
<td>Email Description</td>
<td>:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Net Traffic Fields</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Time</td>
<td>24/08/2015 12:51:09</td>
</tr>
<tr>
<td>Traffic Source IP &amp; Port</td>
<td>[49464]</td>
</tr>
<tr>
<td>Traffic Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Traffic Dst IP &amp; Port</td>
<td>[80]</td>
</tr>
<tr>
<td>Traffic Description</td>
<td>:</td>
</tr>
<tr>
<td>GET/POST URL</td>
<td>:</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>DATE</th>
<th>WHO</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

POINTS TO REMEMBER:

a. Where did the incident occur?
b. Who reported or discovered the incident?
c. How was it discovered?
d. Are there any other areas that have been compromised by the incident? If so what are they and when were they discovered?
e. What is the scope of the impact?
f. What is the business impact?
g. Have the source(s) of the incident been located? If so, where, when, and what are they?
• Incident coordination – identify and manage your tasks
  – List tasks
  – Assign to individuals
  – Track task completion
### Tasks

<table>
<thead>
<tr>
<th>ID</th>
<th>Title</th>
<th>Assigned To</th>
<th>Status</th>
<th>Start Date</th>
<th>Due Date</th>
<th>Priority</th>
<th>Modified</th>
<th>Modified By</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Analyse disk image</td>
<td>Wilson, Ian, VQH1 R</td>
<td>Not Started</td>
<td>18/05/2016</td>
<td>20/05/2016</td>
<td>(2) Normal</td>
<td>18/05/2016 01:38 PM</td>
<td>Scott, M, Matthew, VQH1 R</td>
</tr>
<tr>
<td>10</td>
<td>Isolate host and collect disk image</td>
<td>Scott, M, Matthew, VQH1 R</td>
<td>In Progress</td>
<td>18/05/2016</td>
<td>18/05/2016</td>
<td>(2) Normal</td>
<td>18/05/2016 01:36 PM</td>
<td>Scott, M, Matthew, VQH1 R</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>No.</th>
<th>Date</th>
<th>Time</th>
<th>Event Title</th>
<th>BT CERT Training Cell. Security Through Knowledge.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0</td>
<td>15/03/2016</td>
<td>13:24</td>
<td>1036 - Clem WT Demostation - Code Red</td>
<td></td>
</tr>
<tr>
<td>5.0</td>
<td>15/03/2016</td>
<td>13:24</td>
<td>Send for Closure Approval</td>
<td></td>
</tr>
<tr>
<td>4.0</td>
<td>14/03/2016</td>
<td>13:41</td>
<td>1636 - Clem WT Demostation - Code Red</td>
<td></td>
</tr>
<tr>
<td>2.0</td>
<td>14/03/2016</td>
<td>13:41</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>14/03/2016</td>
<td>13:37</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Event Details:

- **Title**: Clem WT Demostation - Code Red
- **Method of Detection**: Please Select
- **Blackened Ref**: 1001
- **Classification**: BIBS
- **Event Location**: North Star House, North Star Avenue, Sweden, 12B, 120
- **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

---

**Event Status**: Pending
Peer Review

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

## Current User

<table>
<thead>
<tr>
<th>Current Case Status</th>
<th>Current User (Permissions Available)</th>
<th>Shift Leader (Permissions Available)</th>
<th>Reviewer (Permissions Available)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>Open</td>
<td>Open</td>
<td>Open Send for closure approval</td>
</tr>
<tr>
<td></td>
<td>Send for closure approval</td>
<td>Send for closure approval</td>
<td>Send for closure approval</td>
</tr>
<tr>
<td>Send for Closure Approval</td>
<td>Send for closure approval</td>
<td>Open</td>
<td>Send for closure approval</td>
</tr>
<tr>
<td>Closed</td>
<td>Closed</td>
<td>Open</td>
<td>Closed &amp; Reviewed</td>
</tr>
<tr>
<td>Closed &amp; Reviewed</td>
<td>Closed &amp; Reviewed</td>
<td>Open Closed</td>
<td>Closed &amp; Reviewed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Closed &amp; Reviewed</td>
<td>Closed &amp; Reviewed</td>
</tr>
</tbody>
</table>
Post Incident Review

• Write an incident report
  – Capture actions and lessons
  – Presentable and accessible
  – Trustworthy threat intelligence
### Post Incident Review

<table>
<thead>
<tr>
<th>Incident Ref</th>
<th>Date Incident Opened</th>
<th>Date Incident Closed</th>
<th>PRR Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dd/mm/yyyy</td>
<td>dd/mm/yyyy</td>
<td>xxxxxx</td>
</tr>
</tbody>
</table>

#### 2.0 Incident Summary
- High-level summary of incident.

#### 3.0 Impact
- Impact recorded and business impact.

#### 4.0 Communications
- What communications have been sent.

#### 5.0 Process
- What Process & Playbook have been used and how it’s been reviewed.

#### 6.0 Timeline of events

<table>
<thead>
<tr>
<th>Date / Timestamp</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 7.0 Root Cause
- Insert root cause if known.

#### 8.0 Risk Mitigation
- What actions taken to mitigate the impact on the business / service?

#### 9.0 Prevention of Recurrence
- What is the current risk to service / business of recurrence? What actions need to be completed to reduce this?

#### 10.0 Recommendations / Lessons Learned
- Any recommendations or lessons learned for future PRRs.

Important Note: Any recommendations made should be prioritised according to their potential risk to the business for ‘non compliance’ and ‘cost of completion’ (IT known).

#### 11.0 Comments
- Anything worthy of note.
Post Incident Review

IP ADDRESS
This is an “Address” Cybox object.

198.124.185.87
217.12.199.94
185.82.202.170
57.46.131.151
92.222.71.26

DOMAIN NAME
This is a “Domain Name” Cybox object.

cubeccutactioadfe.xyz
haevbasusearcw.kw
pswiiqasnmwcfj.info
cawbdnfolvxlywm.pw
stvknxly.click
chlfseuphityi.ju
paxstynnetylw.info
glulaladfo.pw
nrttxsklqkg.su
cbbeskkgyhf.su
effiap.org
gkikwgtaulfox.org

FILE (Cybox File)
This is a “File” Cybox object.

OTHER
State the IOC and the corresponding Cybox object.

<table>
<thead>
<tr>
<th>IOC</th>
<th>Cybox Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>/userinfo.php</td>
<td>Link</td>
</tr>
</tbody>
</table>
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


• 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

• 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%202013%20%29_1.7.pdf
Questions & Discussion