# Incident Response Team Exercise (IRTx)

RightPoint have appointed a new Chief Security Officer (CSO) to take control of the organisation’s growing cybersecurity requirements.

One of the first tasks the CSO has undertaken was an audit of the organisation’s Security Policy as a whole. The CSO also ordered a risk assessment be conducted.

From these processes, it was found that the organisation does not have a current incident response plan (IRP). The CSO has now drafted an interim plan and now wants security team to evaluate it.

The CSO has specified that the draft IRP be evaluated against the NIST publication 800-61 Computer Security Incident Handling Guide and make recommendations on any changes that may need to be made.

As there are several new security personnel who have recently joined the team, the CSO of RightPoint has decided that it would be a good idea to run an Incident Response Team Exercise (IRTx) as part of the evaluation of the Incident Response Plan and to allow the new members of the security team to oversee the IRP in an exercise environment.

You and the other members of the incident response team that has been contracted by MidTown IT have been tasked with the job of developing and implementing the IRTx.

The CSO has outlined some ideas that the team should consider.

### Objectives of IRTx

The following are the objectives of the IRTx:

1. Assess the effectiveness of RightPoint’s incident handling processes
2. Assess RightPoint’s Incident Response Teams ability to detect and properly respond to hostile or abnormal activity
3. Assess the IRT’s capability to determine operational impacts of cyber-attacks.
4. Expose weaknesses in cyber operations and policies and provide recommendations to rectify.
5. Then IRTx is to be a Red Team/Blue Team/Purple Team exercise.  
   Note: in this exercise, the Red Team role will be taken by the exercises developers (your team.). The Red Team will use a limited number of defined attack methods
6. The IRTx is to be designed to be run for a duration of no more than 2 hours.

### Type of Exercise

The CSO has decided that the IRTx will be a hybrid exercise. A hybrid exercise uses scripted manual injects with real probes/scans and some actual intrusion attempts.

### Virtual Network Scenario

The following is a diagram of how the network could be configured:

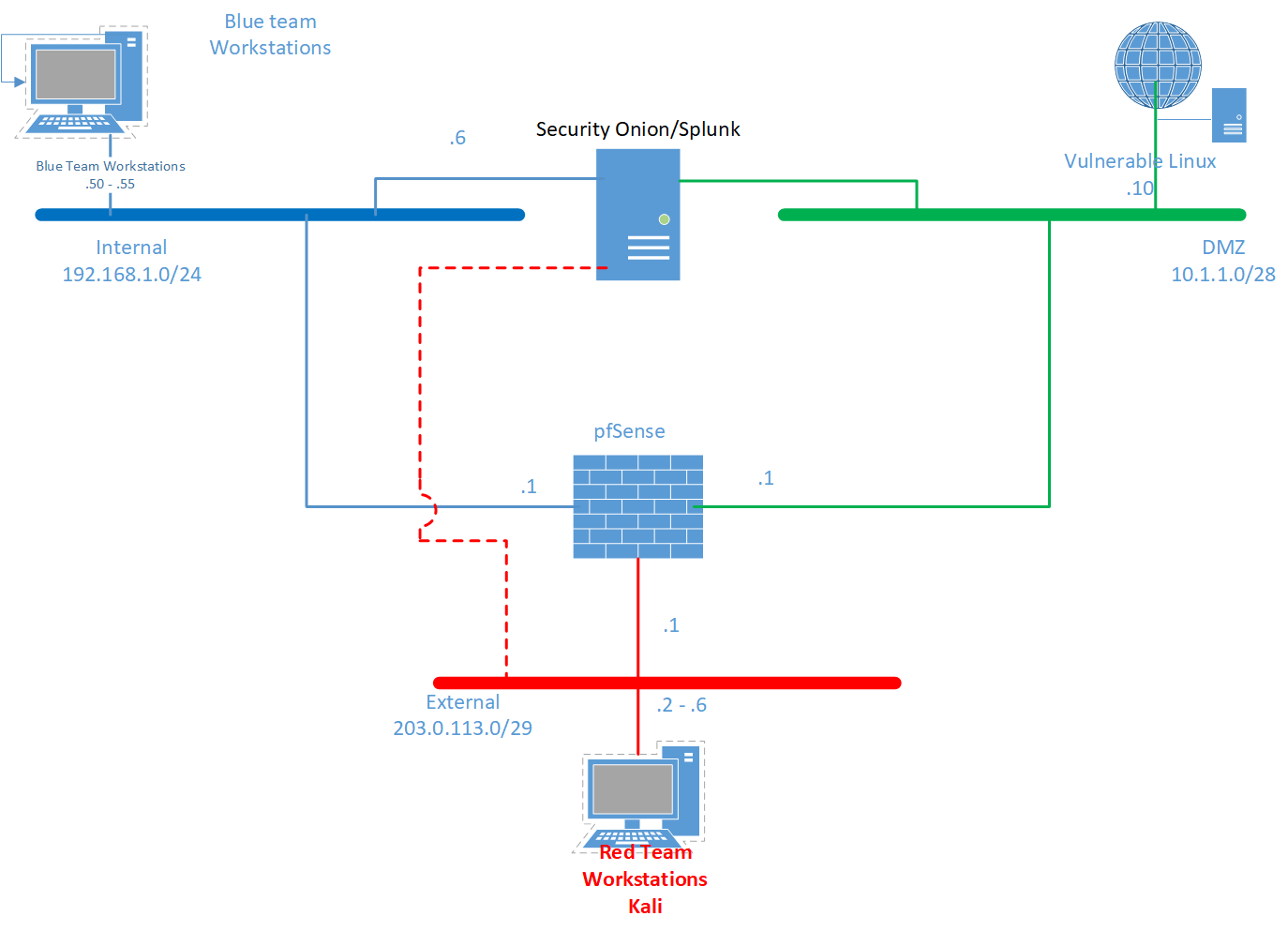


Figure 1 IRTx Virtual Network Scenario

* The number of virtual workstations is dependent on how many members there are on each team. The following are some recommendations:
  + Blue Team
    - Minimum of 2 workstations for analysts
    - 1 workstation for shift supervisor
    - 1 workstation for CSOC manager
    - 1 workstation/server to host the virtual network scenario
  + Red Team
    - Minimum of 2 workstations
  + Observer team
    - 1 workstation
* pfSense could be used as the virtual router/firewall, other options also available such as Cisco ASA\ISR
* Security should be loose to allow for a range of attacks to be implemented with some degree of success. Remember, it is the incident identification, handling, and reporting processes that are being assessed; not the ability to defend.
* Logging should be implemented for each device. Security Onion with Splunk installed is to be used as the IDS/SIEM. You can use ELKS instead of Splunk if you wish.
* Webserver could be DVL, DVWA, or Metasploitable
* Red team will use Kali
* Blue team can use either Linux or Windows
* IP addresses may be changed if required.

### Teams

For this assessment 3 teams are required.

* Each team to have 4 – 6 members
* Each team will develop the following for the IRTx:
  + Red Team playbook
  + Blue team playbook
  + Purple (Observer) Team playbook
* Each team will conduct an IRTx of no more than 2 hours duration

### The IRTx:

* The team running the IRTx will be the Red Team
* One of the other teams will be Blue Team
* Last team will be Purple.
* Each team to be given opportunity to be blue and purple team
* Blue and Purple team playbooks are exchanged at least 1 week prior to the IRTx

### Outline of tasks involved

This project will involve (but not limited to) the following tasks:

1. Developing the project plan  
   This plan is for developing and implementing the IRTx.
   1. Selecting teams
   2. Creating the Project Charter
2. Develop the IRTx
   1. Evaluate existing IRP
   2. Define roles and responsibilities
   3. Identify the business implications of various types of cyber incidents
   4. Define IRTx parameters
      1. Rules of engagement
      2. Red Team playbook created
      3. Blue team playbook created
      4. Observer team playbook created (note: Class teacher is to be included on the observer team)
3. Implement/run IRTx
   1. Create and test a virtual environment as per
   2. Team briefing
   3. Exercise day
      1. Red Team attack
      2. Blue team respond according to IRP
      3. Observer team monitors the blue team and keeps the exercise moving. Injects manual incident scenarios.
4. Reporting
   1. IRTx After Action Evaluation
   2. Project Development/Implementation Report

### Additional information

You are to refer to the appropriate assessment documents for detailed information on assessment tasks and criteria.

You will need to keep in mind that this project is as much about learning as it is about assessment.

### Some useful resources

Project Management

* How to Write the Project Statement of Work (SOW)  
  <https://project-management.com/how-to-write-the-project-statement-of-work-sow>
* How to write a statement of works for any industry  
  <https://www.smartsheet.com/how-write-statement-work-any-industry>
* How to create a Gantt chart in Excel  
  <https://www.smartsheet.com/blog/gantt-chart-excel-b>

Communications Planning

* How to create a project communications plan  
  https://www.smartsheet.com/content/project-communications-plan
* Create a project communications plan  
  <https://www.brightwork.com/blog/create-project-communication-plan>
* Sample communications plan  
  <http://stint-project.net/files/communication_management_plan.pdf>

Meeting documentation

* Three procedures before, during, and after meetings (For bth chaiperson and minute taker)  
  <https://www.cio.com/article/3229972/what-to-do-before-during-and-after-meetings-to-make-them-more-effective.html>
* What is the purpose of meeting minutes  
  <https://www.reference.com/business-finance/purpose-meeting-minutes-6e9de3edcc14f617>
* How to write effective meeting minutes  
  <https://www.wildapricot.com/articles/how-to-write-meeting-minutes>
* How to develop an effective meeting agenda  
  <https://www.thebalancecareers.com/how-to-develop-an-effective-meeting-agenda-1918731>
* How to write an agenda for a meeting  
  <https://www.wikihow.com/Write-an-Agenda-for-a-Meeting>

Status Report

* The ultimate status report checklist  
  <https://www.projectmanager.com/blog/project-status-report-checklist>
* Your project status report checklist: What to include when you report to stakeholders  
  <https://www.softwareadvice.com/resources/project-status-report-checklist/>
* Weekly status report template  
  <http://d2myx53yhj7u4b.cloudfront.net/sites/default/files/IC-Weekly-Project-Status-Report-Template.xltx>

Developing an incident response exercise

* NIST 800-61 - Computer Security Incident Handling Guide  
  <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>
* Cyber Exercise Playbook (This one is used extensively)  
  <https://www.mitre.org/sites/default/files/2022-09/pr_14-3929-cyber-exercise-playbook%20.pdf>
* If you can get hold of the following publications, they could be of help:
  + Blue Team Field Manual (Alan J White, Ben Clark
  + Red Team Field Manual (Alan J White, Ben Clark)  
    Both of the above books are available from Amazon.com
* NIST 800-86 Integrating forensic techniques into incident response  
  <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>
* Guide for designing cyber security exercises  
  <https://www.researchgate.net/publication/228953270_Guide_for_designing_cyber_security_exercises>
* NIST 800-84 Guide to test, training, and exercise programs for IT plans and capabilities  
  <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf>
* A brief idea about tabletop testing. This has a cyber attack demo.  
  <https://tools.databarracks.com/dr-tabletop-simulation/index.html>
* Running an effective incident response tabletop exercise  
  <https://blog.rapid7.com/2017/07/05/running-an-effective-tabletop-exercise/>
* 4 cyber incident scenarios you should exercise and test  
  <https://deltarisk.com/blog/4-cyber-incident-scenarios-exercise-test/>
* Incident Response workflow and tips  
  <https://www.process.st/checklist/it-security-incident-response-plan/#introduction>
* Incident Response Playbook designer  
  <https://www.incidentresponse.com/playbooks/>
* Incident Handling Annual Testing and Training  
  <https://www.sans.org/reading-room/whitepapers/incident/incident-handling-annual-testing-training-34565>

pfSense (Firewall +)

* Download ISO  
  <https://www.pfsense.org/download/>
* Download pfSense ova appliance (virtual machine)  
  <https://sourceforge.net/projects/virtualappliances/files/Appliance/Network/pfSense-2.1-amd64.ova/download>
* pfSense documentation  
  <https://www.netgate.com/docs/pfsense/>

Security Onion

* Security Onion Download and Documentation  
  <https://github.com/Security-Onion-Solutions/securityonion/>

ELK Stack resources (Open Source SIEM)

* The complete guide to the ELK Stack  
  <https://logz.io/learn/complete-guide-elk-stack/#intro>
* ELK Stack VM – Bitnami (Virtual Appliance)  
  <https://bitnami.com/stack/elk/virtual-machine>
* Bintami ELK Stack - Getting started  
  <https://docs.bitnami.com/virtual-machine/apps/elk/>

Data Dumps/Simulated traffic

The following are sites where you can download different log files.

* SecRepo.com – Samples of security related data  
  <http://www.secrepo.com/>
* NetReSec – Publicly available PCAP files  
  <https://www.netresec.com/?page=PcapFiles>
* Bro Browser  
  <https://www.netresec.com/?page=PcapFiles>