Open Source Incident Management Tool for CSIRTs

Adli Wahid
Head, Malaysia CERT (MyCERT)
CyberSecurity Malaysia

Agenda

- About MyCERT
- Where do incidents come from?
- Open Source Incident Handling Tool
- Conclusion

About MyCERT

1997	CyberSecurity Malaysia
Malaysian Internet Users	15 staff

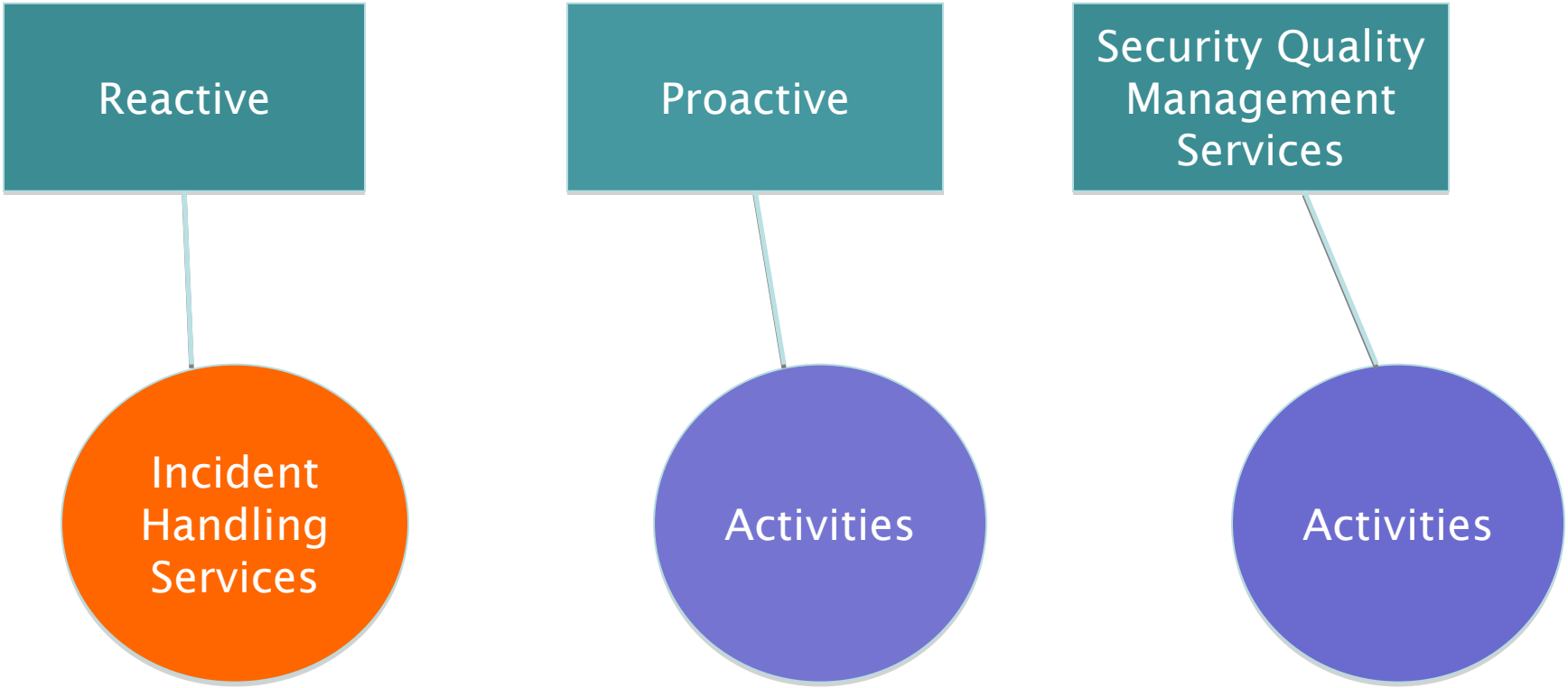
MyCERT's Services

Cyber999

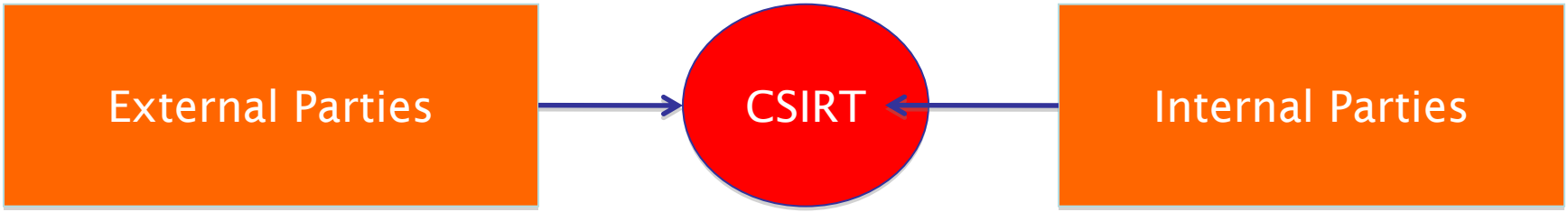
Cyber Early Warning Research

National CERT & Global Emergency Co-ordination

Possible Services of CSIRT



Where do incidents come from?



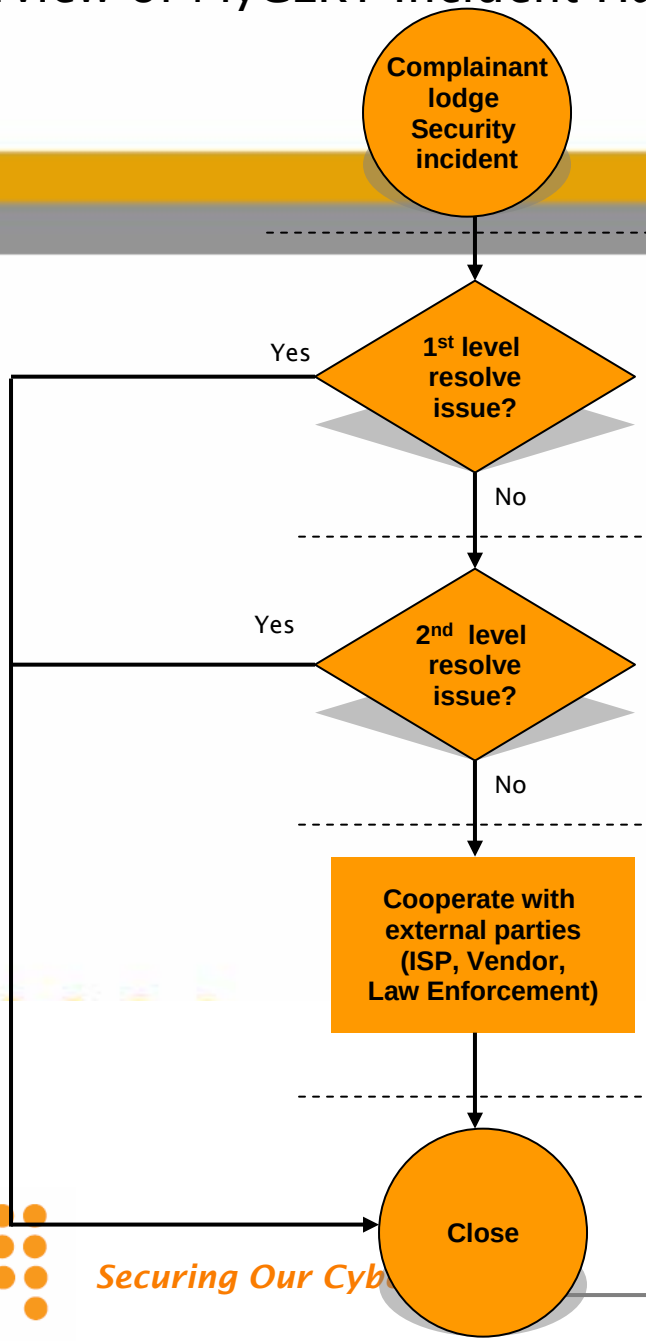
Example of Incidents

- Defacement
- Host being used to send spam
- Host connected to a bot command & control
- Scanning activities from your network
- Etc – Internal incidents

SOPs

- Standard Operating Procedures
- Different for different incidents
- Shows workflows and
- Response Time (SLAs)

Overview of MyCERT Incident Handling Process



- Complainant lodge report to MyCERT via phone, fax, sms and email:
  - cyber999@cybersecurity.org.my or
  - mycert@mycert.org.my

- Analyze the report and verify sufficient information is available to proceed
- Provide information and guide complainant in next course of action
- Ensure compliance to service level:
  - Destructive or Criminal* incidents – 24 -48 hours
  - Spam/harrassment – next working day

- Follow up with complainant until case is closed
- Analyze artifacts, logs, intelligence gathering, etc
- Provide solution/advise/recommendation based on analysis conducted

- Cooperation in assisting complainant to lodge official reports with respective law enforcement.
- Assist law enforcement & ISPs in gathering and preserving evidence
- Escalate to vendor should assistance is needed in getting the solution or the case is vendor-related

- Feedback to complainant and close the case

Securing Our Cyb

** Destructive/Criminal Incidents include: Intrusion, Denial of Service, large*

Artefacts Handling

Logs

Binaries

ETC

Screenshots

The tool that you need

Incident Management Tool

Requirements

- Unique ticketing, tracking
- Escalation – more than one user
- Artifacts handling
- Secure communication
- Database of contacts

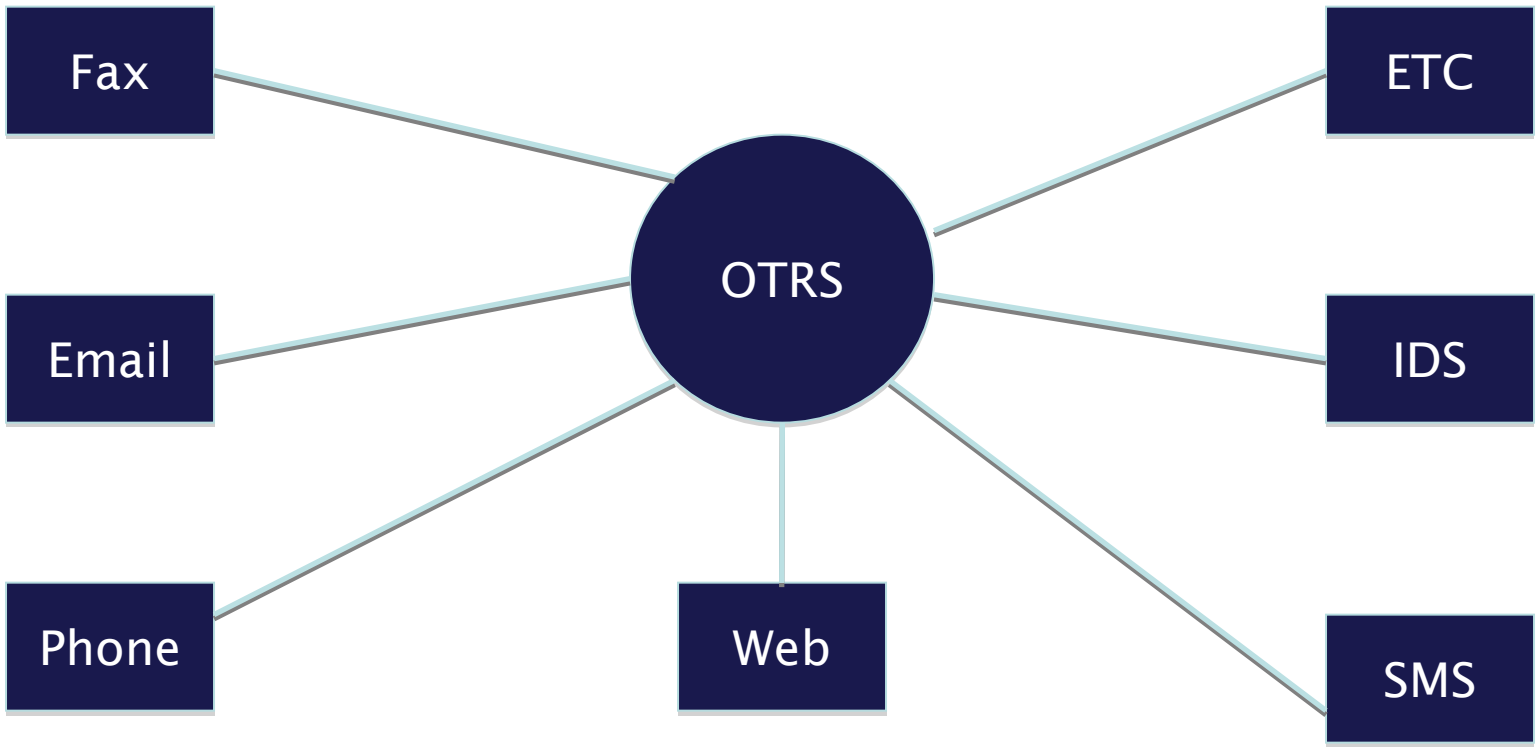
Open Source Options

OTRS

RTIR

AIRT

Incident Reporting Channel



OTRS Modules

- Incident tracking module
- Authoring tools for advisories
- Vulnerabilities database
- Artifact database
- Contacts database
- Ticket module
- WebWatcher
- Call module
- IDMEFConsole

Screenshots – OTRS in Action

Conclusion

- People, Process, Technology makes up CSIRT
- You need tools to support incident handling activities
- Choosing the right tool for your work is important

- Thank You!
- adli@cybersecurity.org.my