Building a CSIRT team in South Africa

- How do you succeed ?
- What information risks do we address?
- Benefits and Challenges?

CSIRT Model

- Why Form an Incident Response Team?
- Ability to Coordinate
- Ability to Work Proactively
- Expertise
- Hybrid model
- Centralized core team
- Specialists in steering committee

CSIRT constituency

- Internal
- External
- Other CSIRT, FIRST members
- Government

Tools

- Work flow management system
- Response Analyzes + Investigation tools
- Digital forensics
- Net Flow
- Incident and Even Monitoring Tools
- Specialized

Skills

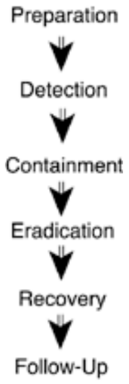
- Information Security
- Data Mining
- Digital Forensic
- Client relationship skills

Identification of Events and Incidents

- Internal data flow
- E-Mail internal,external
- security,event and incident information systems
- External CSIRT teams
- external entities, industry risk forums,other organizations

Six-Stage Methodology for Incident Response

- The PDCERF incident response methodology



Preparation

Detection

Containment

Eradication

Recovery

Follow-Up

Signs of an Incident

- Computer used to access other systems in the DMZ?
- Users download sensitive source code or information?
- Users upload malicious code or modify source code?
- Computer accessed in any way other than FTP?
- Did the access occur at a higher privilege level?
- Customer data present in the DMZ + accessible from the web server compromised?

Challenges in setting-up in our region

- Connectivity limitations
- Cross borders operations (legislation, communications, timezones)
- Authorities co-operation in the event of a cyber crime, or incident
- Maturity of current legislation
- Dispersed organization, business unit across 10+ different country’s
- Training of 1st responder’s in our org

Accreditation

- Transits training
- Sponsorship
- FIRST
- Growth of other players in our region
- 3 other Banks + Banking Risk Commitee

FIRST Teams around the world

CSIRT future growth

- Setting-up more CSIRT’s at other financial organizations
- Industry focused CSIRT for the Banking industry
- Training getting more individuals trained
- Real life scenario testing

Questions?