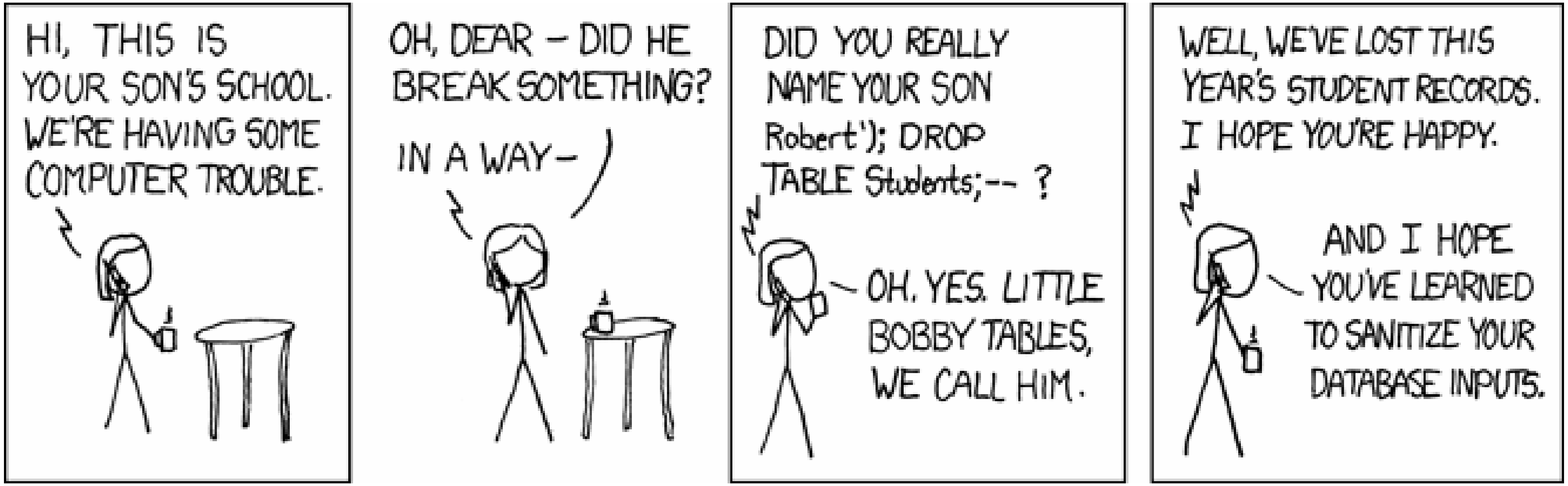
TeliaSonera


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Distributed security incident response organization

”A.K.A. TeliaSonera subCERT organization”

TeliaSoneraCERT CC

- **80-s Occasional computer crime investigations**
- **1993 Central Investigation Unit**
- **1996 Team Data**
- **1998 TeliaCERT**
- **1999 TF-CSIRT (former EuroCERT)**
- **2000 FIRST membership**
- **2001 TF-CSIRT Level 2 (accredited)**
- **2002 Initiator of Swedish CERT-Forum**
- **2003 Changed name to TeliaSoneraCERT CC**

Role and Purpose

- The main mission of TS-CERT is **to manage threats and attacks against computers and computer networks that support TeliaSonera's business operations and information assets**. The purpose is to minimize damage and disruptions caused by IT security incidents.

- TS-CERT is a **Coordination Centre for handling IT security incidents at corporate level**. TS-CERT coordinates the handling together with appointed security incident handling teams within the business units. TS-CERT takes an **active** role in security incident investigation and analysis.

- TS-CERT is the main recipient of IT security incident reports within TeliaSonera.

- The responsibility also includes **following up IT security within the TeliaSonera Group** by conducting vulnerability assessments, penetration tests and enforcing applicable policies. This is done in close co-operation with CIO.

- TS-CERT represents TeliaSonera in the international Forum of Incident Response and Security Teams (FIRST) and the European TF-CSIRT (Task Force Computer Security Incident Response Teams).
  TSS-Abuse represents TeliaSonera in E-Coat.

Areas of operations

- Incident Handling and coordination
  - Emergency response
  - Lead and coordinate subCERT organization
  - Provide assistance to subCERTs
    - Computer forensics
    - Artifact analysis
- Follow-up
  - Coordinate and conduct penetration tests
  - Conduct security analysis of critical systems
- Information coverage and distribution
- Advice and guidance
  - Training
  - Participation in projects
  - ”Consultants”

Identified issues

- Company present in many countries
  - Large distances
  - Different legislation and regulation
  - Different types of business

- Lack of presence
  - Security on a strategic level vs operations
  - Corporate culture
  - “Talk around the coffee table”

- Rapid changes
  - Organizational
  - Technical

- Other problems
  - Internal requirements
  - Financing

Pre-requisites for SubCERT in TeliaSonera

- Roles
  - Team owner
  - Team leader
  - Team member
- SubCERT statement
  - Purpose and goal (formally signed by management)
  - Constituency and Demarcations
  - Roles and responsibility
  - Reporting
  - Staffing and financing
  - Co-operation
- Code of Ethics and Code of Practice
- Acceptance of common procedures
  - Triage
  - Escalation Procedures
  - Incident Tracking System
  - E-mail templates, Report templates, Incident Flows
- Training
- Tools

Training

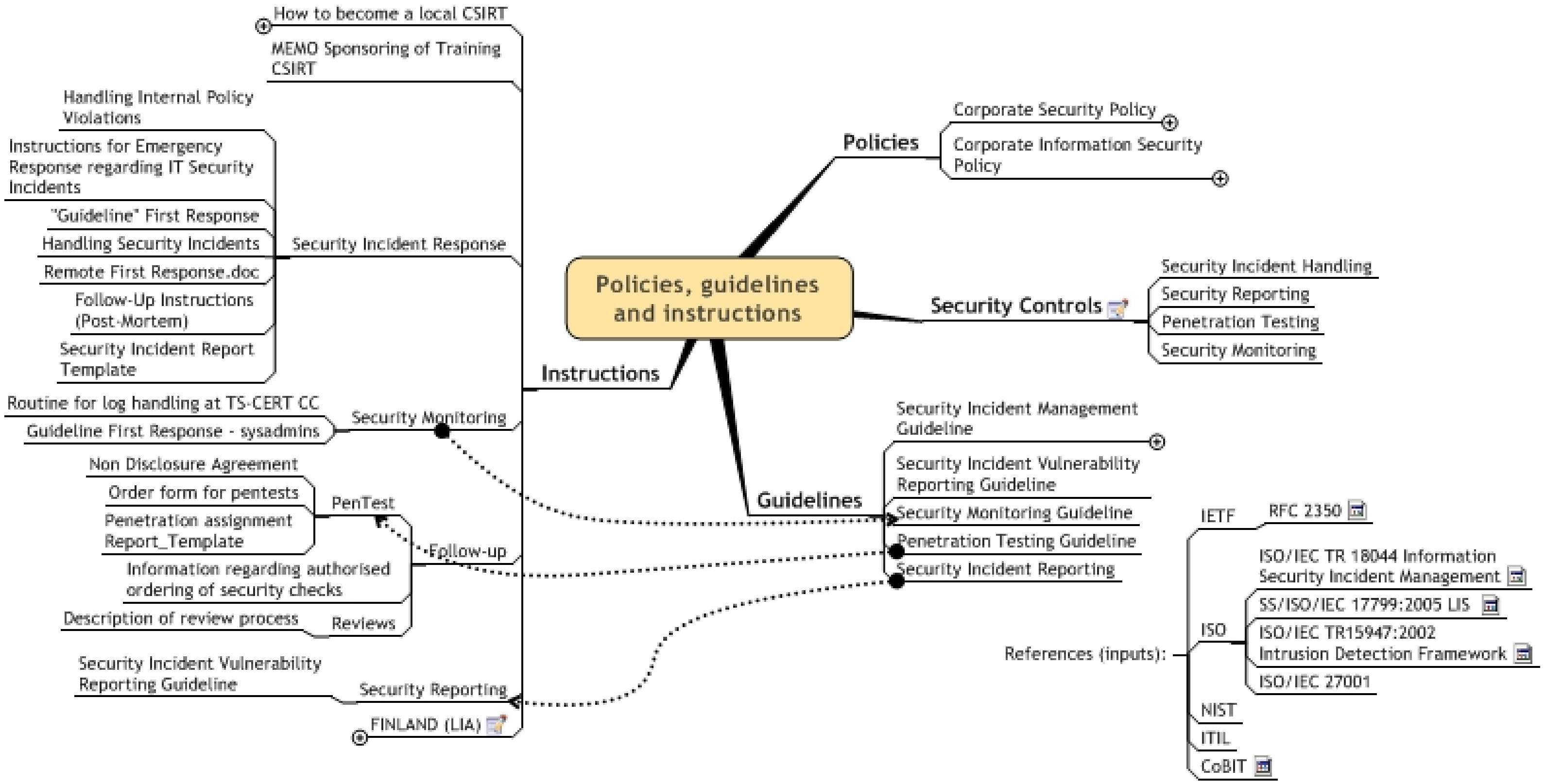
- Basic Education (by TS-CERT)
  - TSG Incident Organisation (2 days)
  - Walk-by-hand Incident Training (5 days)
  - Establishment of own SubCERT (10-15 days)

- Technical Training (by SANS Institute)
  - Hacker Techniques, Exploits and Incident Handling System Forensics, Investigation and Response

- Manager's Education (by TF-CSIRT and CERT/CC)
  - TRANSIT Course
  - CERT/CC

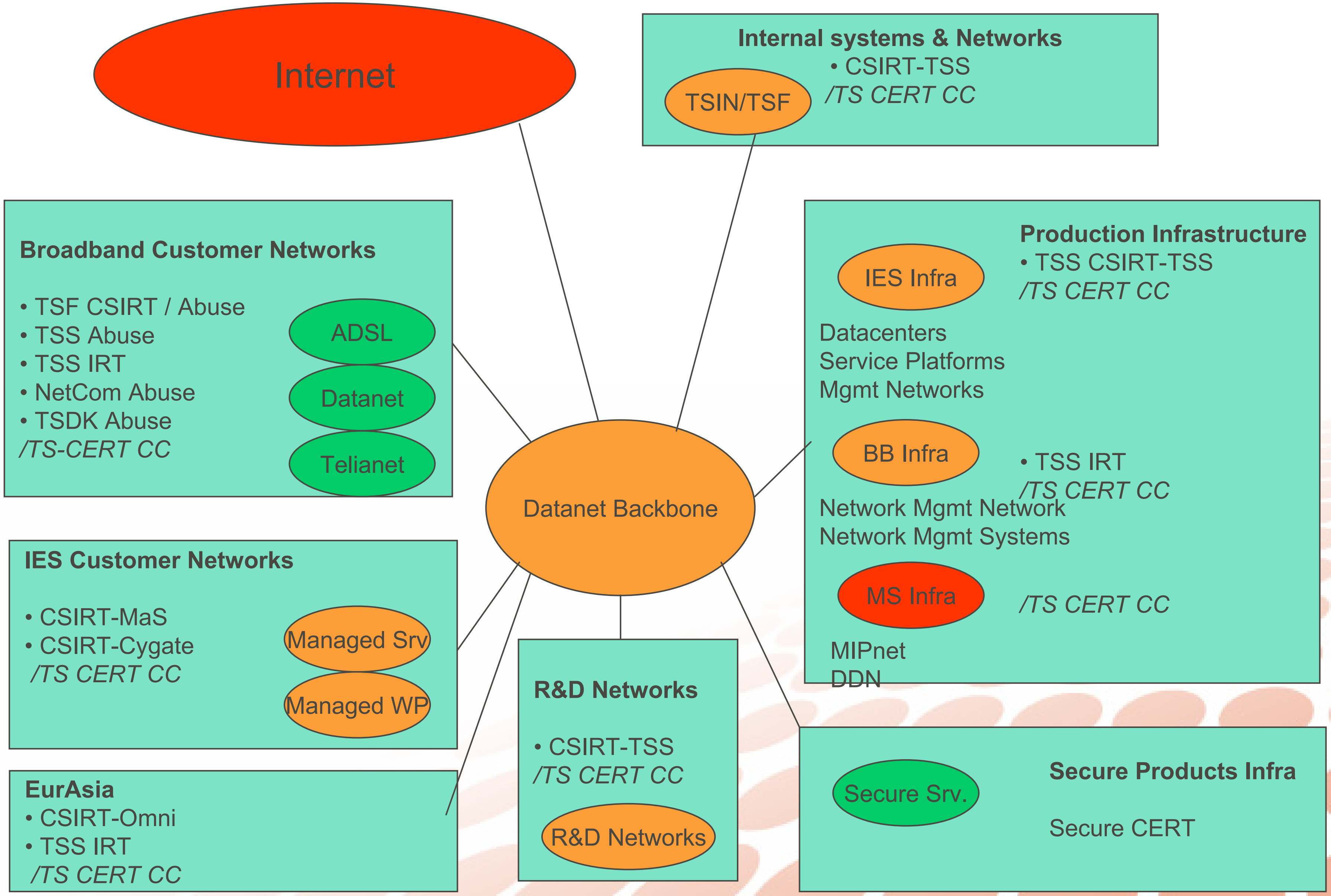
- Optional Training (by SANS Institute and CERT/CC)
  - Auditing Networks, Perimeters & Systems (SANS T7)
  - Intrusion Detection In-Depth (SANS T3)
  - Computer Security Incident Handling for Technical Staff (CERT/CC)

Available policies, processes and instructions



Policies, guidelines and instructions
Policies
Corporate Security Policy
Corporate Information Security Policy
Security Controls
Security Incident Handling
Security Reporting
Penetration Testing
Security Monitoring
Guidelines
Security Incident Management Guideline
Security Incident Vulnerability Reporting Guideline
Security Monitoring Guideline
Penetration Testing Guideline
Security Incident Reporting
References (inputs):
IETF
RFC 2350
ISO
ISO/IEC TR 18044 Information Security Incident Management
SS/ISO/IEC 17799:2005 LIS
ISO/IEC TR15947:2002 Intrusion Detection Framework
ISO/IEC 27001
NIST
ITIL
CoBIT
Instructions
How to become a local CSIRT
MEMO Sponsoring of Training CSIRT
Security Incident Response
Handling Internal Policy Violations
Instructions for Emergency Response regarding IT Security Incidents
"Guideline" First Response
Handling Security Incidents
Remote First Response.doc
Follow-Up Instructions (Post-Mortem)
Security Incident Report Template
Security Monitoring
Routine for log handling at TS-CERT CC
Guideline First Response - sysadmins
Follow-up
PenTest
Non Disclosure Agreement
Order form for pentests
Penetration assignment Report_Template
Information regarding authorised ordering of security checks
Reviews
Description of review process
Security Reporting
Security Incident Vulnerability Reporting Guideline
FINLAND (LIA)

TS subCERT organization (based on constituency)



Internet

Internal systems & Networks
- CSIRT-TSS

/TS CERT CC

TSIN/TSF

Broadband Customer Networks

- TSF CSIRT / Abuse
- TSS Abuse
- TSS IRT
- NetCom Abuse
- TSDK Abuse

/TS-CERT CC

ADSL

Datanet

Telianet

Datanet Backbone

Production Infrastructure
- TSS CSIRT-TSS

/TS CERT CC

IES Infra

Datacenters
Service Platforms
Mgmt Networks

BB Infra

- TSS IRT

/TS CERT CC

Network Mgmt Network
Network Mgmt Systems

MS Infra

/TS CERT CC

MIPnet
DDN

IES Customer Networks

- CSIRT-MaS
- CSIRT-Cygate

/TS CERT CC

Managed Srv

Managed WP

R&D Networks

- CSIRT-TSS

/TS CERT CC

R&D Networks

EurAsia
- CSIRT-Omni
- TSS IRT

/TS CERT CC

Secure Products Infra

Secure CERT

Secure Srv.

The role of TSCERT CC

- Define incident response policies, procedures and related documentation
- Coordination both internally and externally
- Assistance to subCERTs
- Quality assurance
- Special cases
  - Requiring specialized knowledge
  - Handed off to Law Enforcement
  - Other cases within our constituency
- Analysis
  - Of security incidents
  - Of new technology
- Training of
  - subCERTs
  - other units

Pro’s and con’s

“Pros”

- Close to operations and development
- Local knowledge (language, differences in work & social culture)
- Clearly defined constituencies
- Easier to adopt to organizational changes
- The cost for the incidents will affect the correct business unit

”Cons”

- Central CSIRT can become unknown within the organization
- Central CSIRT don’t get enough cases
- subCERTs don’t get the support needed for its operation
- Reporting is hard to make perfect
- Daily communication
- Common workspace

Questions, comments …

TeliaSonera

Additional resources/information

- CERT/CC
  - Organizational Models for Computer Security Incident Response Teams
  - Handbook for Computer Security Incident Response Teams (CSIRTs)
- TF-CSIRT Starter kit
- TSCERT CC
  - ts-cert@teliasonera.com