Recent History

May 2010: official rebranding of CERT-DEVOTEAM
- Merge of Security Watch and Advisories and Incident Handling groups
- CSIRT activities for the whole DEVOTEAM group (24 countries) and customers
- Rebranding → CERT©/CC, TF-CSIRT, ENISA

Previously known as APOGEE SecWatch
Timeline

1996: Start of the security watch activity for banks
   - APOGEE Communications

1998: Monthly security watch reports

1999: Daily security alerts "VTS Alertes"

2000: Incident Handling & Forensics

2001: Daily "SecWatch", SOC

2003: DEVOTEAM Group

2005: Anti-phishing

2006: Weekly "WISec"

2007: Listed at TF-CSIRT

2010: Daily "SecPointers" → "SecAlert(e)s"

2011: Accredited at TF-CSIRT
Our overall CSIRT activities

CERT-DEVOTEAM Activities

Reactive Services
- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

Proactive Services
- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services
- Risk Analysis
- Business Continuity & Disaster Recovery Planning
- Security Consulting
- Awareness Building
- Education/Training
- Product Evaluation or Certification

Service Offered in Cooperation With Other Entities Within Group

Not Offered Service

Illustration: CIRT services by category. Source: Carnegie Mellon
Sample recent activities

- Security Watch
  - Security Alert Watch: Weekly and/or Daily reports and alerts
  - Security Technical Watch: Monthly reports on methods, products, tools
- Anti-fraud
  - Phishing, compromise
- Incident Handling
  - Incident analysis, incident response
- Investigations
  - Forensics
- Security assessments
- Research
- CSIRT set-up
  - Support, mentoring
Cooperation with other countries (mostly anti-phishing)

- Support of DEVOTEAM entities
  - AT, CZ, DK, NO...

- While handling incidents
  - National and GOV CERTs/CSIRTs
    - AU, BE, CA, CH, DE, FI, FR, HU, IE, IL, MA, MT, NO, RO, UK, US, ZA, EU, UN, NATO
  - Banks, Travel…
    - DE, FR, NL, UK, US, ZA…
  - Hosters & ISPs
    - AT, CA, CZ, DE, DK, FR, GR, IL, JP, PE, UK, US, ZA…
  - Research
    - CA, FR, US, ZA

- Not easy with some other countries
Contacts

http://www.cert-devoteam.com

Contact / Legal Information
- RFC 2350

Archives
- Archives since 1999