Incident Management
ITU Pillars & Qatar Case Study

Michael Lewis, Deputy Director

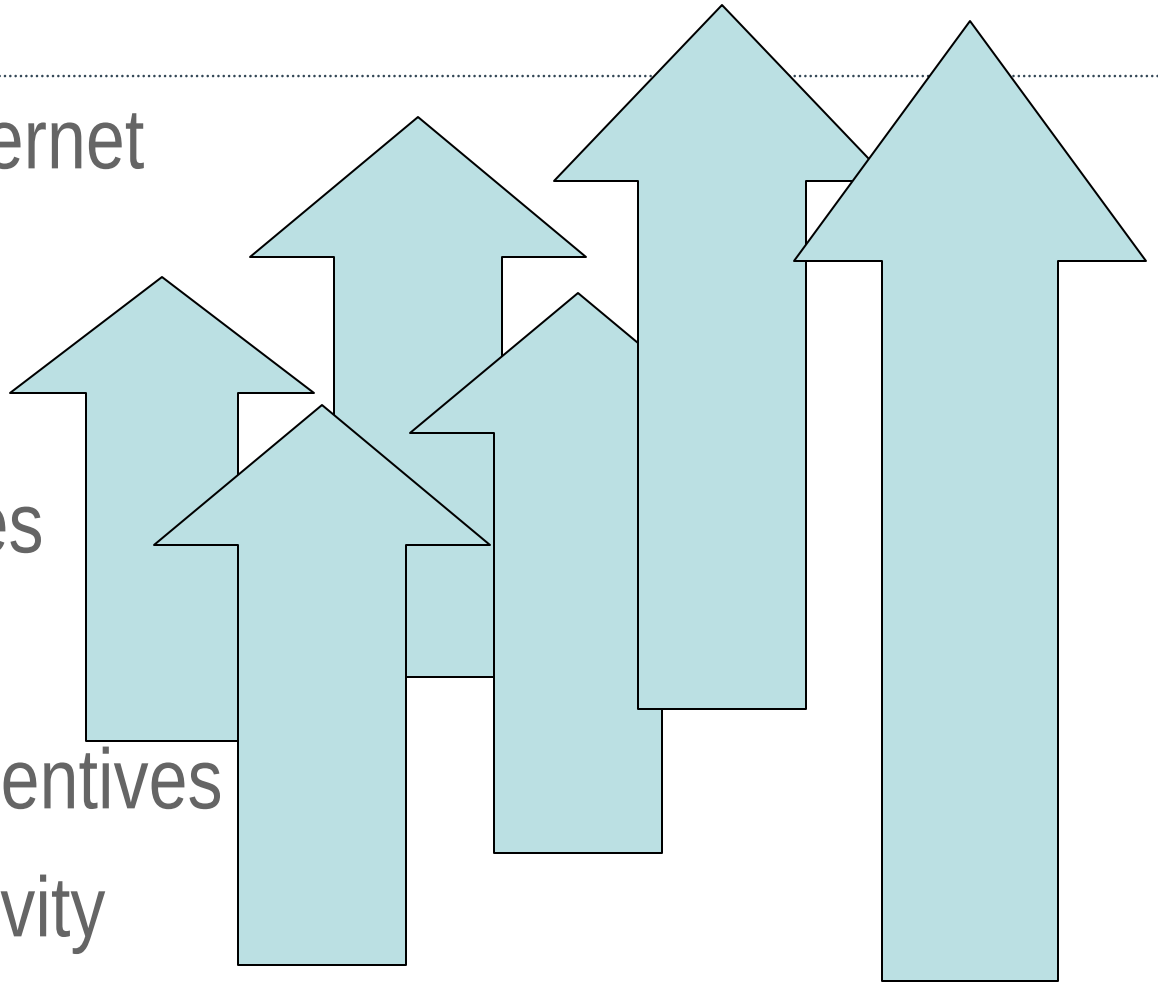
Thanks …

- To the ITU for sponsoring the initiative – ictQATAR has worked closely with the ITU-D since the project's inception, from the WTDC '06 Doha conference to the regional meeting in February
- To the BCDE of Australia for hosting the event
- And to my Aussie friends for the cultural tutorial!

G'day!

General Trends ...

- Users on Internet
- Computers
- Devices
- Vulnerabilities
- Exploits
- Financial Incentives
- Criminal Activity



The Economic Issues of CyberCrime

- Barriers to entry are low
  - resources are essentially free (!)
  - technical requirements are modest
- Risks for criminals are low, Rewards high!
  - Returns are tantalizingly large
  - Opportunities grow with continued E-volution of services
  - Difficult to trace and attribute
  - Investigation costly in time, resources, money
- CRIKEY! Cybercrime is a growth industry!

Coordinating a National Approach to Cybersecurity

ITU Pillars of Cybersecurity as a Reference Point

providing the collected “best practices” of the community

- Developing a National Cybersecurity Strategy
- Establishing National Government-Industry Collaboration
- **Creating National Incident Management Capability**
- Deterring Cybercrime
- Promoting a National Culture of Cybersecurity

The Approach in Qatar

Q-CERT was established in December 2005 as the National CERT for the State of Qatar.

- A project of the Supreme Council for Information and Communications Technology – ictQATAR
- In partnership with the CERT Coordination Center of Carnegie Mellon University
- A member of regional & international communities of information security teams (GCC, AL, FIRST)

The program is organized into three major groups …

Outreach, Awareness, & Training

- Conduct Information Security training
- Formalize incident response through building organizational CSIRTs
- Host workshops & conferences
- Organize public awareness campaigns
- Cooperate with schools & universities
- Provide forums for discussion and training

Critical Infrastructure Protection

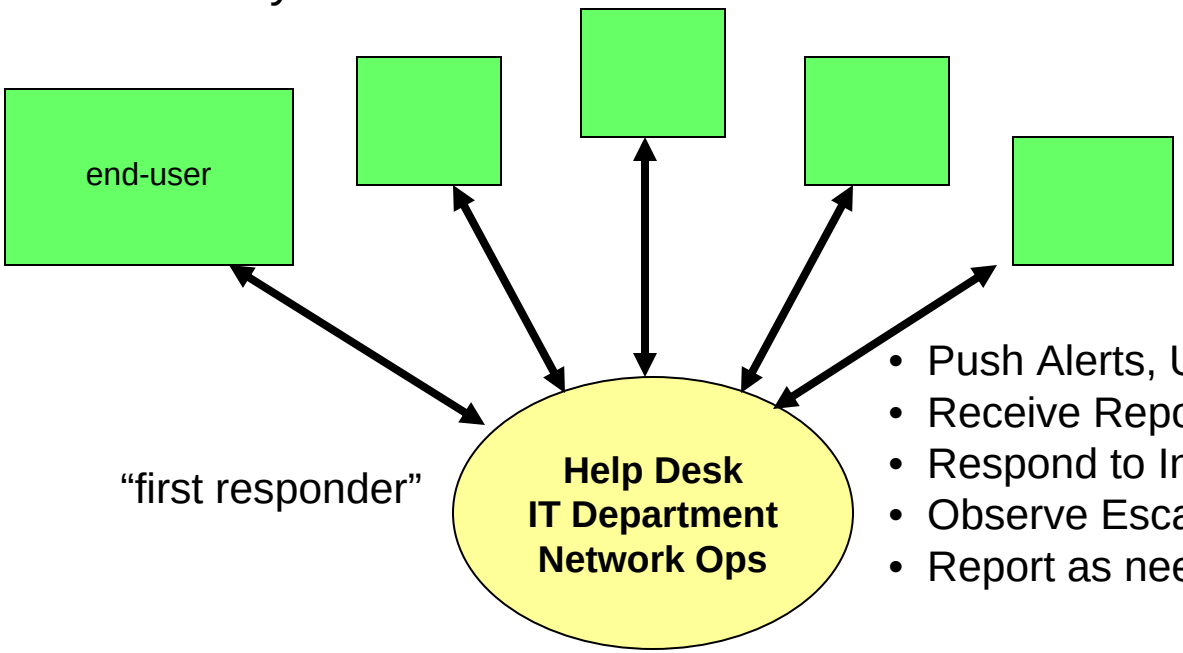
- Lead the National Information Assurance Framework project (in alignment with ITU Framework initiative)
- Shape national info-sec mandates and policies on the use of protocols & international standards
- Work with Critical Sector Organizations to improve their security postures – banking & finance, oil & gas, government, ict, etc.
- Foster creation of sector working groups

Incident Management

- Distribute Alerts
- Collect Reports
- Coordinate Incidents
- Conduct Incident Analysis
- Provide Cyber Forensics Training & Resources
- HoneyNet, Malware, & Botnet Eradication
- and the Cyber Security Network

“Front-Line” Incident Response

Who do they call?



“first responder”

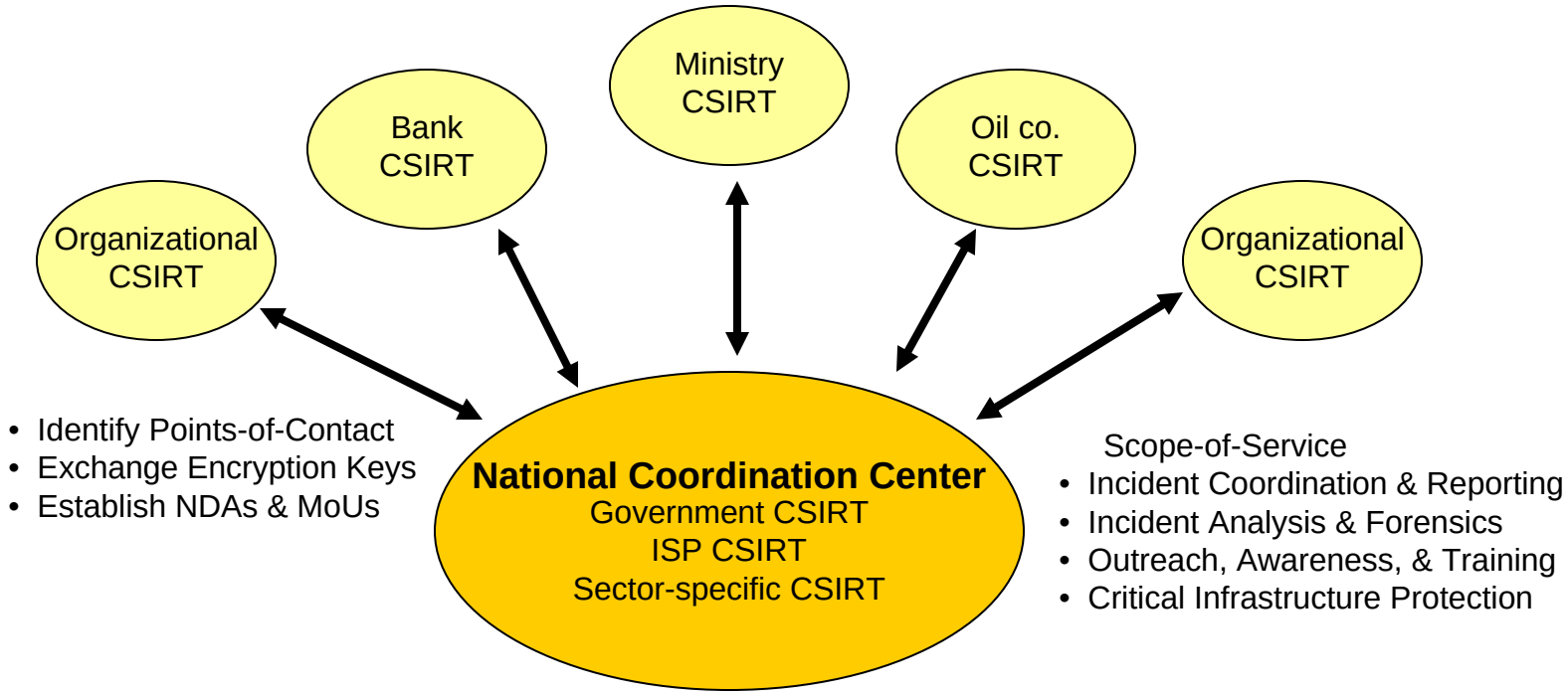
Help Desk
IT Department
Network Ops

- Push Alerts, Updates, Patches
- Receive Reports
- Respond to Incidents!
- Observe Escalation Procedures
- Report as needed to national center

An organizational CSIRT

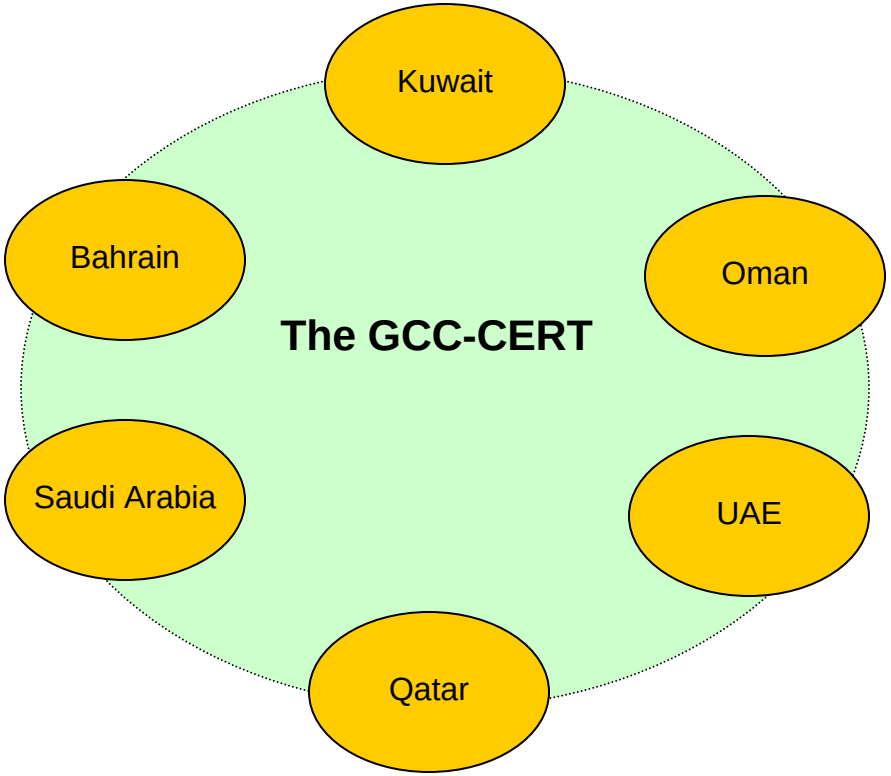
to formalize internal incident response

National CSIRT



The National Cyber-Security Network

Regional Cooperation

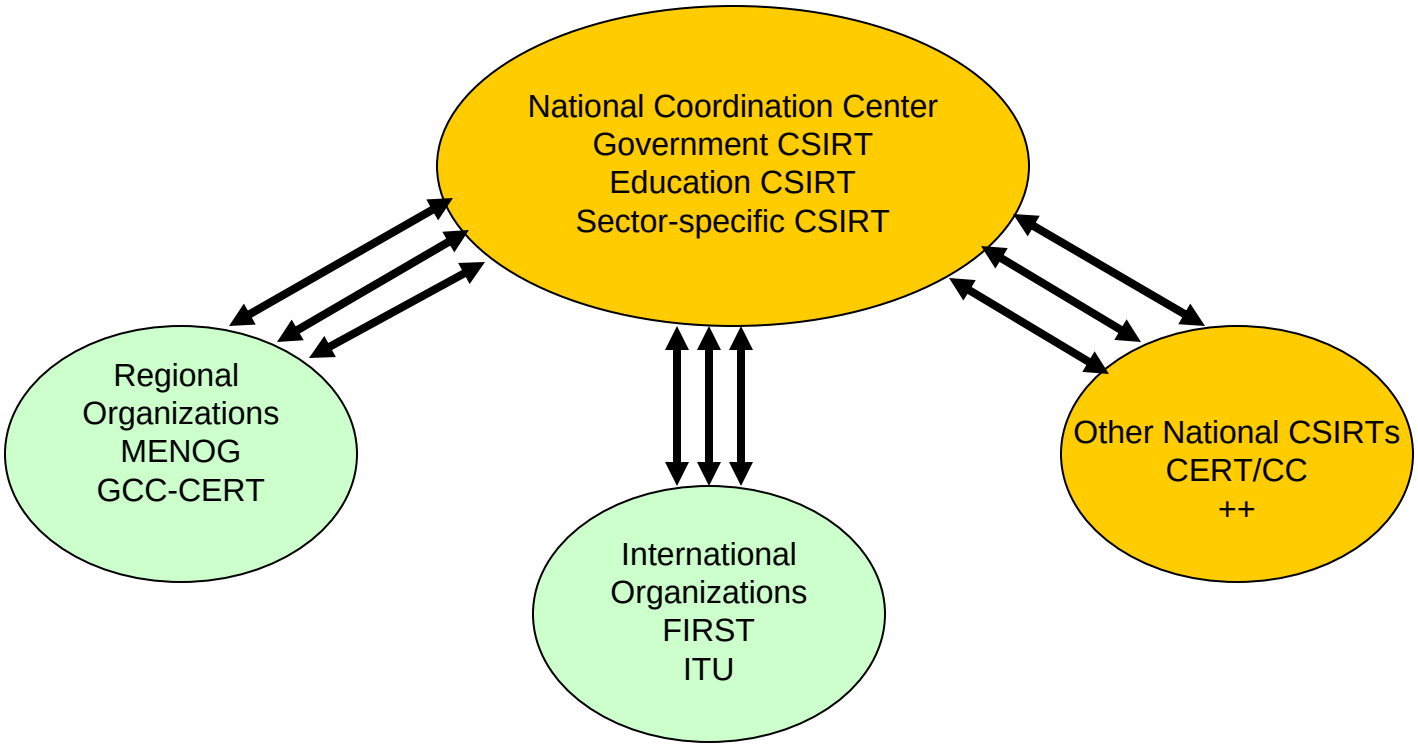


- Establish PoCs
- Exchange Keys
- Data Exchange Agreements
- Conduct Technical Meetings

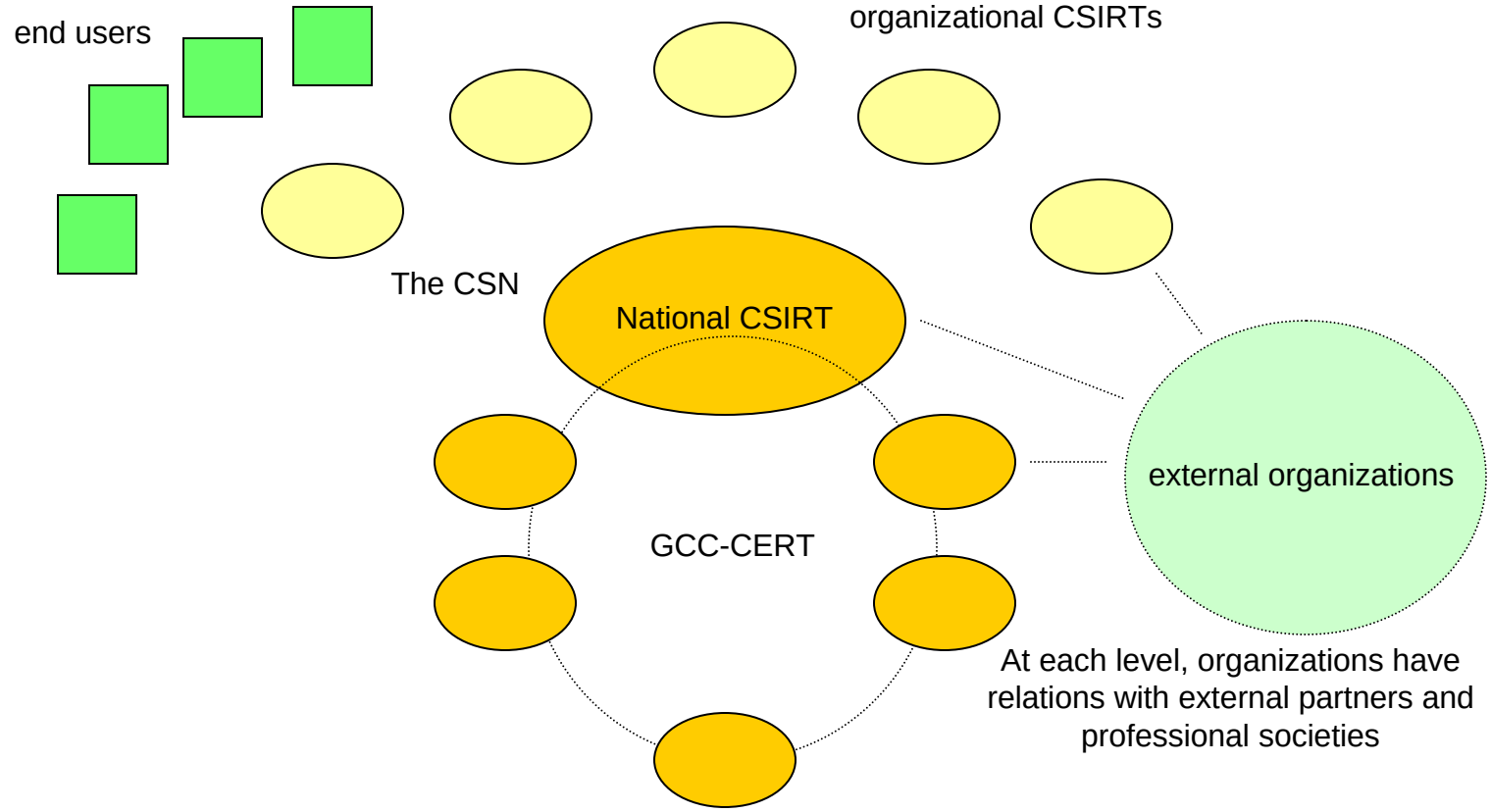
GCC-CERT – Milestones

- April 2006 — Concept Paper on regional GCC-CERT
- May 17 — GCC calls for creation of national CERTs & authorizes the GCC-CERT
- June 12-13 — QATAR convenes a workshop on Building National CERT programs
- July 18-19 — QATAR hosts a second regional workshop
- Nov - Dec — Country visits & National CERT workshops
- 2007 — Legal considerations & working meetings
- May 2008 — Formally constituted as a GCC committee

External Relations

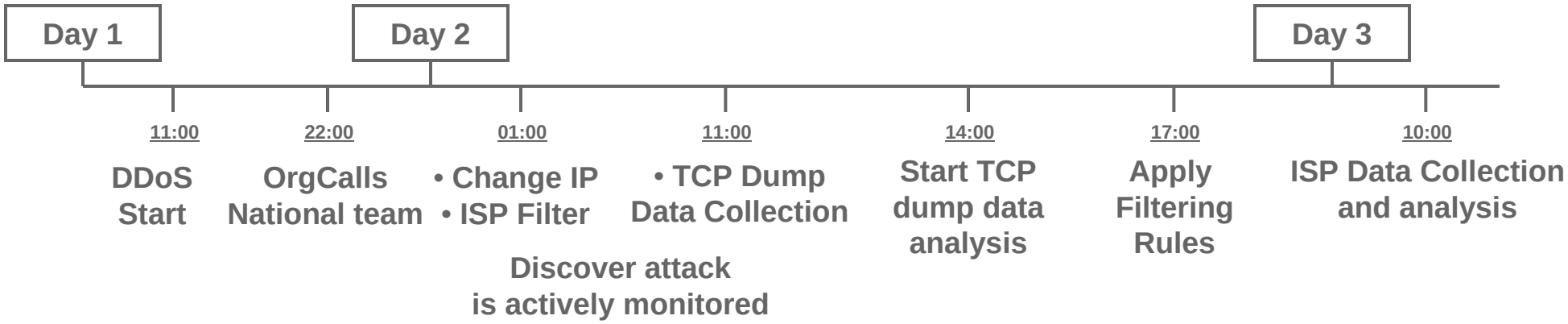


The Full Picture

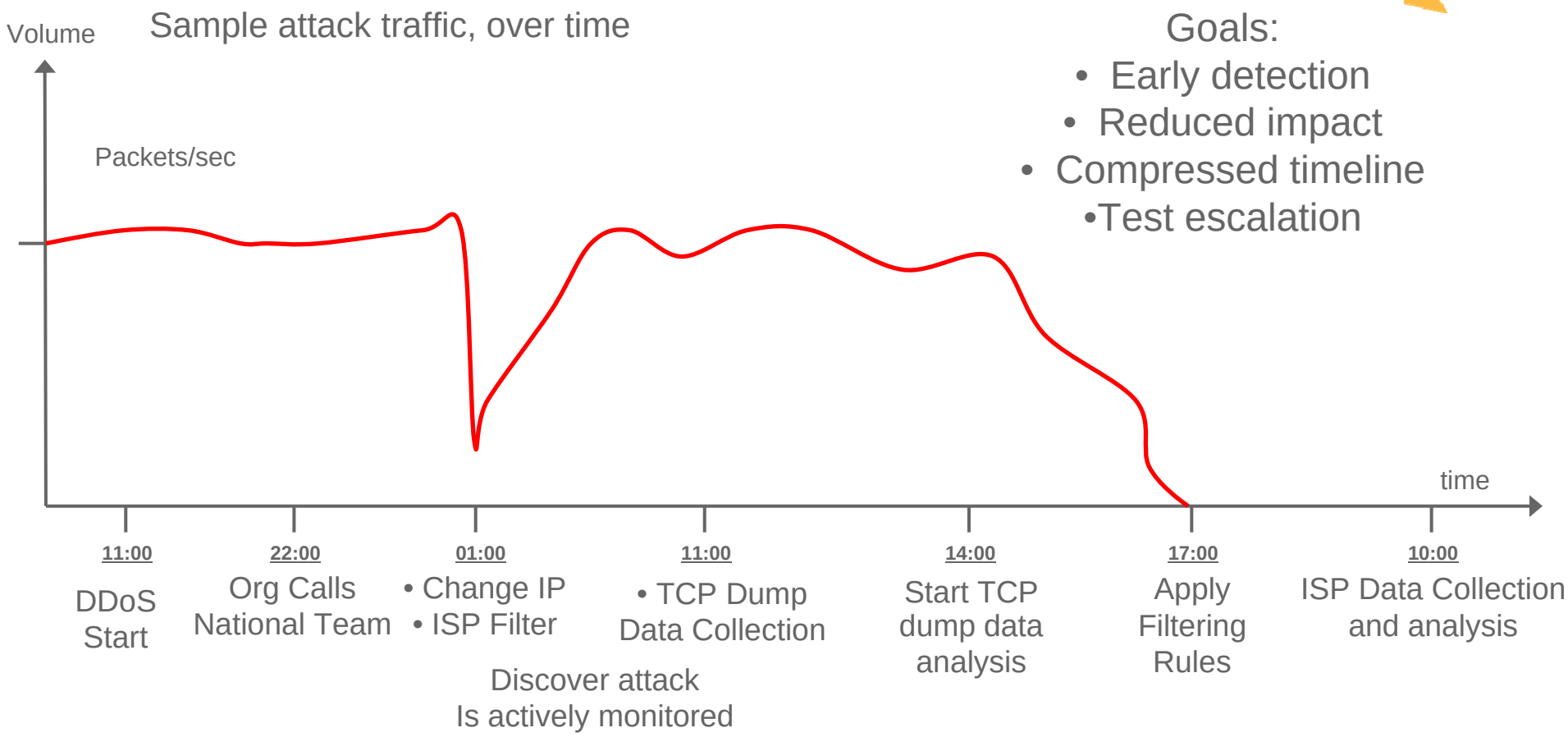


Incident Management

An example for our constituents
a genericized DDOS attack
events over 48 hours



Impact of Mitigation Strategies



Goals:

- Early detection
- Reduced impact
- Compressed timeline
- Test escalation

Aftermath Questions

- What can be done to improve detection and response?
- When did the attack actually start? When did it stop? Was there a discernible pattern that might help future early detection strategies?
- Review the impact of mitigation strategies – what worked? What didn't?
- Review the sequence of deploying the mitigation strategies – was order important?
- Was the proper escalation procedure observed?
- Were the right partners involved?

NYA1 Under Revision

Nora Yousef al-Abdulla; 08.06.2008

General Questions

- Are there “default” strategies that can be designed in advance and rapidly deployed for different types of incidents?
- If so, what is the threshold/trigger for their activation?
- What are the respective responsibilities of targeted site/ISP/CSIRT?
- Are there liability issues involved, regarding intervention and advice?

Building a Culture of Cybersecurity

- Identify constituents & counterparts – national, regional, international
- Establish trusted relations and secure communications
- Conduct regular, targeted events to share experience and build human networks

  … Recent events from Q-CERT …

June 10-11

Q-CERT continued its support of the emerging Info-Sec community of Doha by participating in the Doha Information Security Conference (DISC), organized by the WTC of Qatar.

June 12

Q-CERT presented a workshop at Qtel, the primary ISP of Qatar, to further ongoing technical cooperation.

Q-CERT as the National CSIRT
Trends Briefing
Botnet Overview
Botnet Technical Assessment
Botnet Eradication Project
Incident Analysis & Cyber Forensics

June 15

Q-CERT hosted a meeting of the regional GCC-CERT, which formally convened as a committee of the GCC Ministry of Post, Communication, and IT

June 18

Q-CERT and Microsoft co-hosted a signing ceremony at the Doha Sheraton to formally establish Q-CERT as a member of the Microsoft Security Program.

Microsoft

June 19

Q-CERT hosted a meeting of the Qatar Information Security Forum (QISF) on the topic of CyberCrime Legislation.

June 22-27

Q-CERT served as a gold sponsor for the FIRST annual membership meeting in Vancouver

FIRST™
Improving Security Together
2008 SPONSOR

June 24-29

Q-CERT conducted a four-day workshop “Information Security for Technical Staff” targeting critical-sector organizations.

June 30 – July 3

Q-CERT senior technical staff spent a week at the CERT/CC for training in the administration and use of the CCAP forensics analysis system.

July 1

Q-CERT organized and presented a workshop on National CSIRTs and Regional Cooperation for the Arab League in Cairo.

www.qcert.org

Thank You