How to get ISPs to collaborate with National CERTs

Haythem EL MIR

Technical Manager, Positive Technologies

Introduction

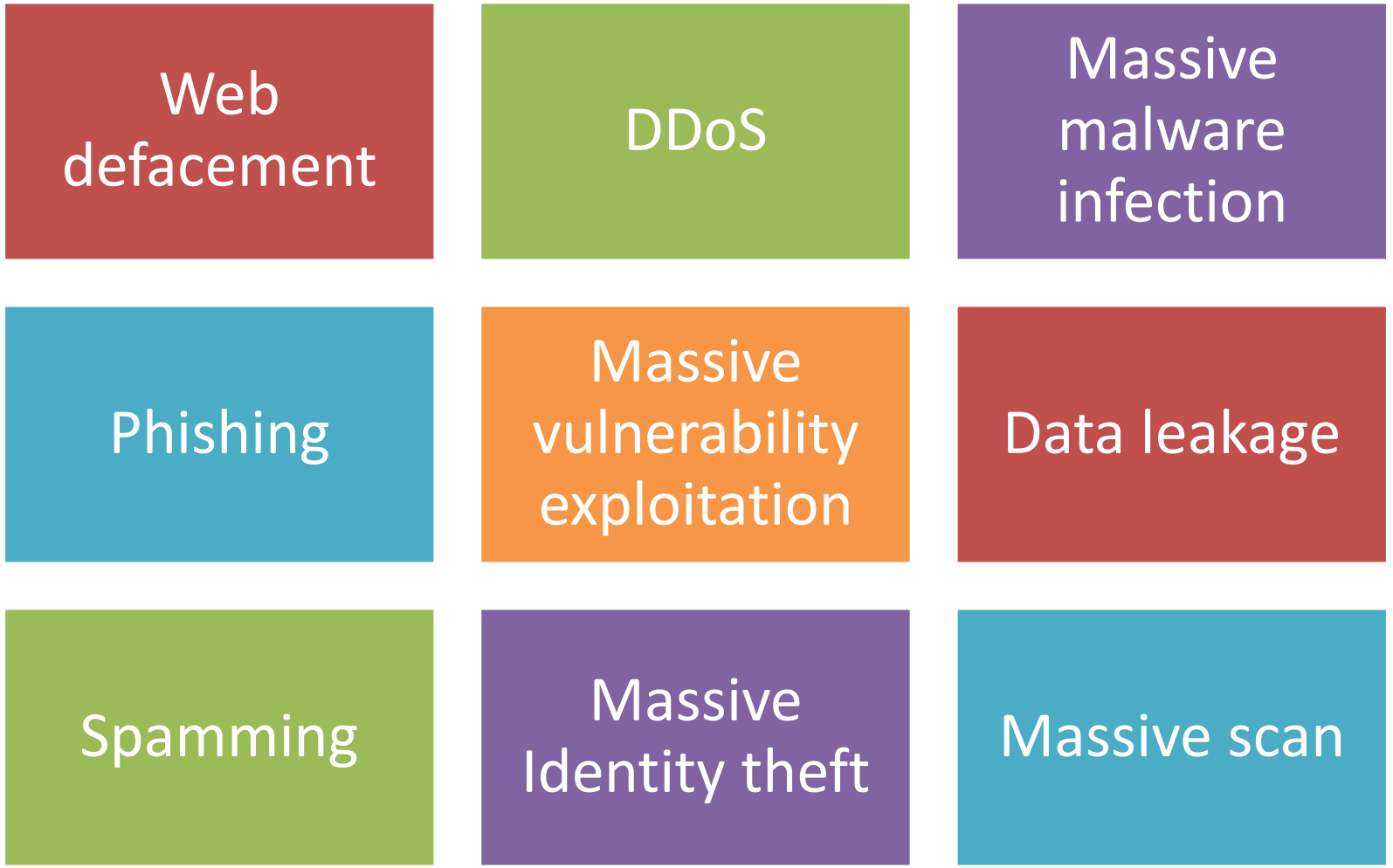
CERT

- A specialized entity for incident and emergency response, ensuring preventive and proactive services.
- A CERT is acting at a national level to secure the cyberspace, and assist internet users to handle incidents and to protect their assets.
- A trusted Point of Contact for national and international cyberspace stakeholders

ISP

- Providing all internet related services, including Security. The first Point of Contact for their customer in case of incident.
- Well-positioned to contribute improve cybersecurity
- A trusted Point of Contact for their customers

Incident Response Coordination



Introduction

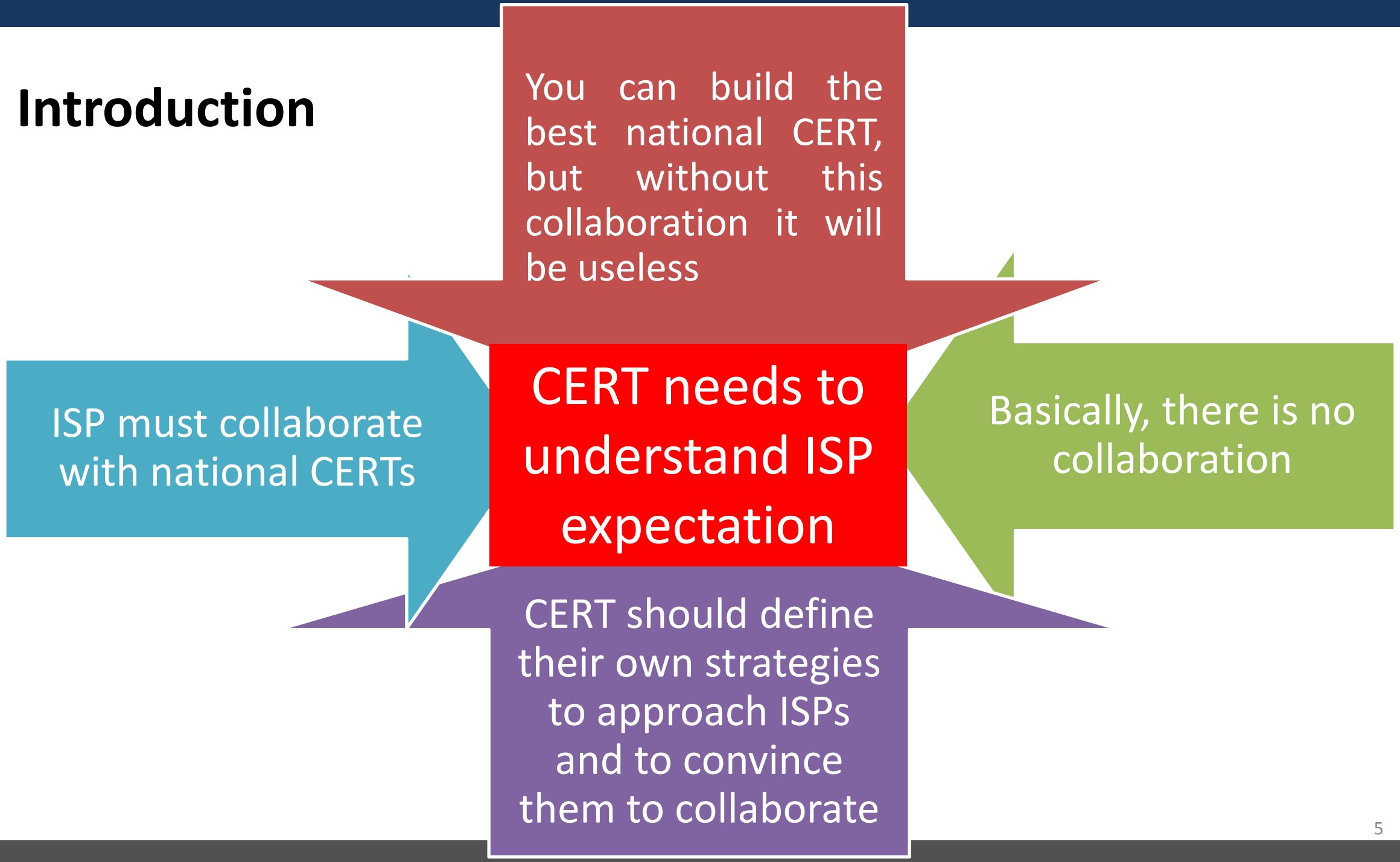
We are all facing the same problems

We need to collaborate

National CERT should be the key player and the key coordinator

National CERT should be integrated in their ecosystem

Introduction



How to get ISPs involved?
What CERTs need to do?

1 Select carefully your target

- Identify the key stakeholders and focus all your efforts on them (the biggest, the most critical, the most targeted, the easiest to convince, etc.)
- The others will follow,
- There will be some good and positive partners and there will be some others considering themselves as better than you,
- For those who will resist, just wait for some critical incidents and they will come.

2 Show your expertise: you are the expert

- ISPs must consider CERT as an expert and focused team ready to help them to respond to their incidents,
- CERT must spend all their efforts to develop their technical skills and to get ready to any kind of incident while ISP cannot afford this investment,
- ISP will trust this technical expertise and will start to rely n the CERT,
- To show the expertise: workshop, site visit, labs, success stories, procedures, etc.

3 Help ISPs to respond to their incidents

- If needed send them a team on site,
- Offer them a premium 24/7 service,
- Provide a dedicated incident reporting (online ticketing systems, dedicated email, etc.)

4 Help them to detect their incidents

- Run a dedicated monitoring and threat intelligence,
- Alert them in case of attacks: web defacement on their customers websites, infected users, phishing, etc.
- Help them to deploy monitoring systems:
  - IDS,
  - Honeynet,
  - DNS sinkhole,
  - Netflow,

Share information

give than ask

Gather information coming from:

- Public sources,
- Other CERTs,
- Other Honeynet,

- Share information about current threats:
  - vulnerabilities,
  - exploits on the wild,
  - Malware infection,
  - Cyber-threats
  - Detected attacks (Web defacement, Malware infection, Spam, DoS/DDoS, Phishing, etc.)

6 Offer free assistance

- Security assessment after incident closure,
- Assistance to secure and implement recommendations and best practices,
- Help them to deploy security solutions (Firewall, IDS, WAF, VPN, etc.) mainly from open source,
- Help them to develop cybersecurity awareness program for their staff and for their customers.

7 Train and do cyber exercices

- Train them on incident response,
- Train them on coordination procedures,
- Organize periodic cyber exercises/ Cyber drill,
- During incident response ask your team to explain and to do some transfer of competence,
- Share your experience with them.

8 Ensure a continuous communication

- Make sure that you have a good communication with ISPs especially during emergencies,
- Maintain efficient communication channels between teams: email and phone mainly,
- Hold a meeting with top management and periodic ones with technical teams, do technical workshops/forum, etc.

9 Show your engagement to secure their data

- Insist on applying security controls like:
  - Email encryption,
  - Securing your network,
  - Physical security,
  - Data protrction,
  - Etc.
- Make sure they are informed about your security policy and recommend them to adopt similar controls.

10 You are the trusted Point of Contact

- Develop your international collaboration network and present yourself as the main Point-of-Contact with foreign entities,
- As a trusted PoC you can easily help them to solve their problems: incident, blacklisting, etc.
- Being member of FIRST, OIC-CERT, AfricaCERT, etc. can help to achieve it.

What to avoid?

- Don‘t report incident to their top management,
- Don’t ask them to spend a lot of money,
- Don’t be pretentious,
- Don’t tell them you are mandated by law and the should comply,
- Don’t be late in case of emergencies.

Conclusion


1
2
3
4
5
6
7
8
9
10
Build and maintain trusted and
A win-win relationship


Thank you for
your attention