CERT md

RENAM
RESEARCH & EDUCATIONAL NETWORKING ASSOCIATION OF MOLDOVA

CyberSecurity at RENAM

Ecaterina Matenco

9-10 February, EaPConnect CyberSecurity Workshop

RENAM & CERT Overview

National Research and Educational Network of Moldova since 1999.

MD-CERT is a center of internet security expertise, located at the RENAM.

MD-CERT starts in January 2007

Region Info

On the current moment we have 2 CERT in Moldova:

- MD-CERT that handles incidents in R&E network – www.cert.md
- CERT.GOV.MD is governmental CERT – www.stisc.gov.md/ro/cert-gov-md

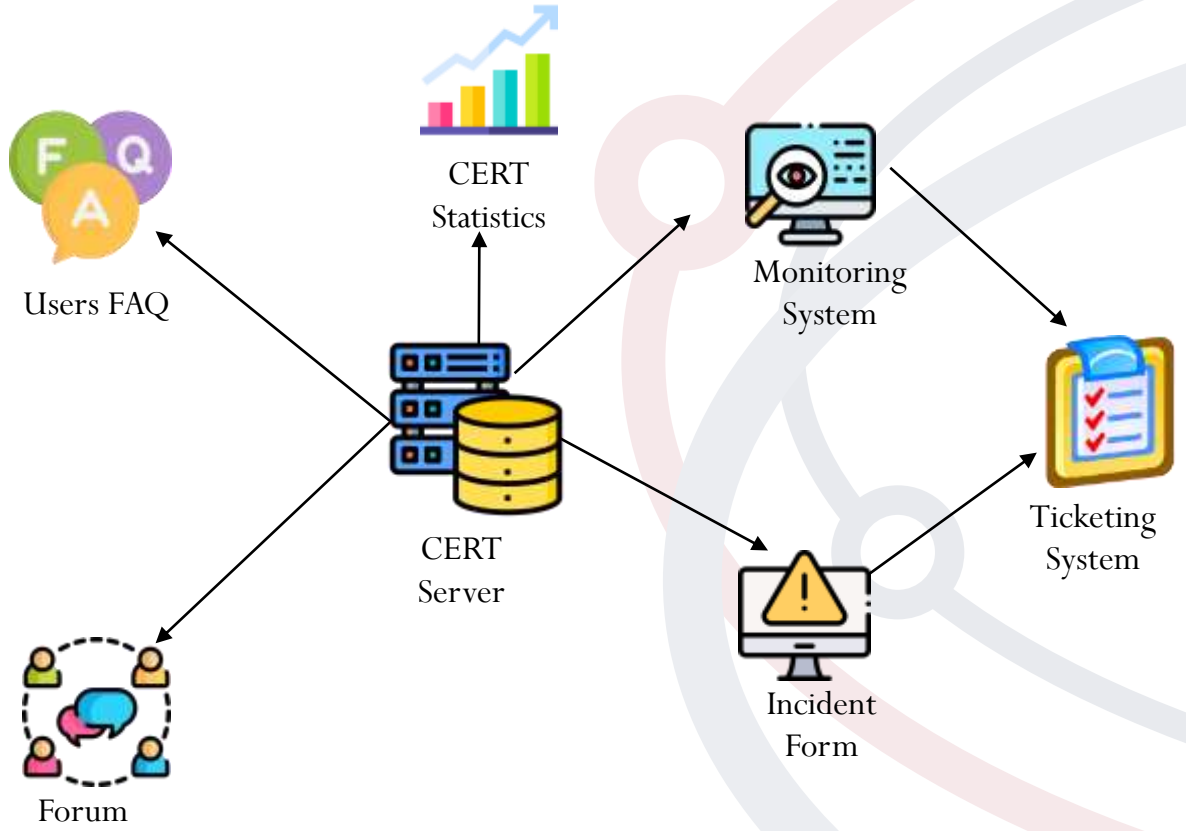
About CERT MD

- We study internet security vulnerabilities, research long-term changes in networked systems, and develop information and training to help to improve security in R&E network in Moldova.

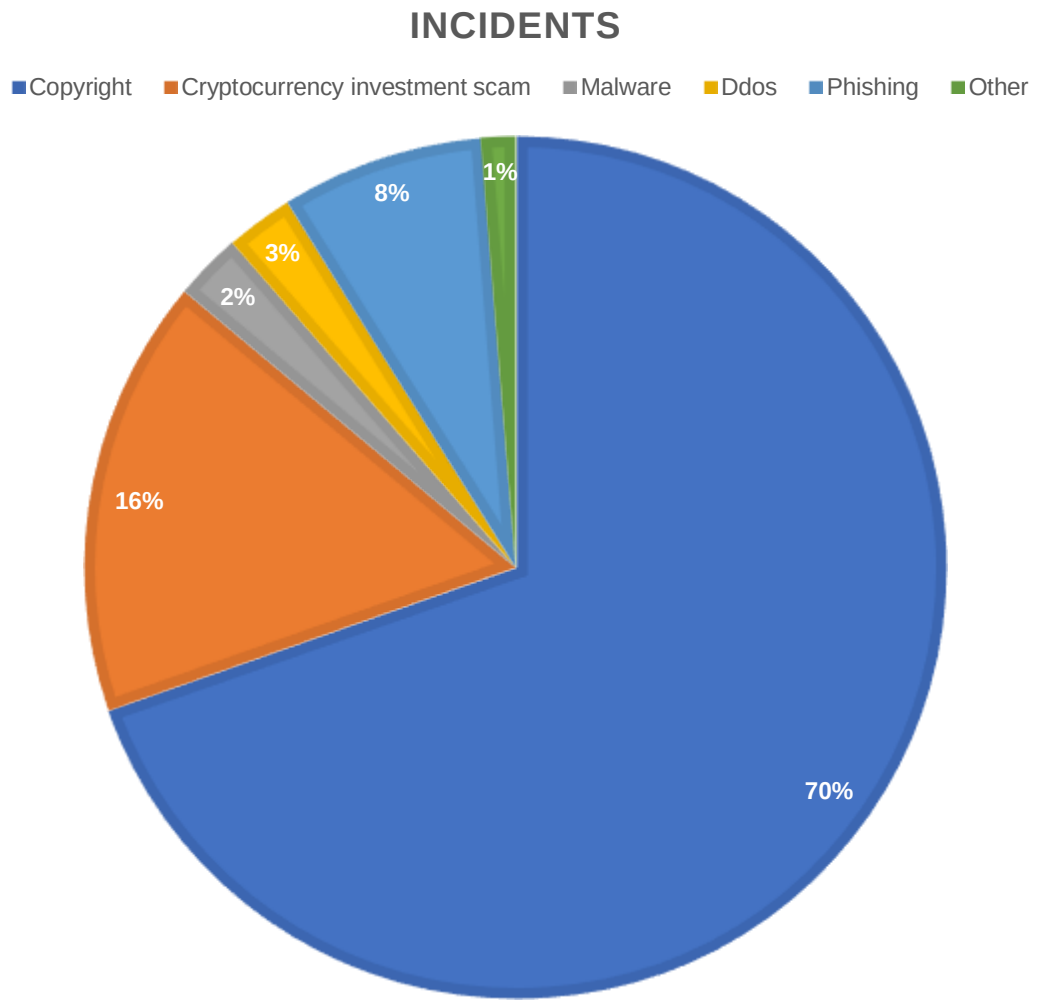
- MD-CERT was finished the registration procedure by Trusted Introducers and become TI-Listed CERT.

CERT-MD Services

- Incidents Handling
- Monitoring
- Distributing Information about Security vulnerabilities.
- Consulting
- Network Audit
- Web Resources Audit
- DDOS Protection



Incidents Statistics 2021

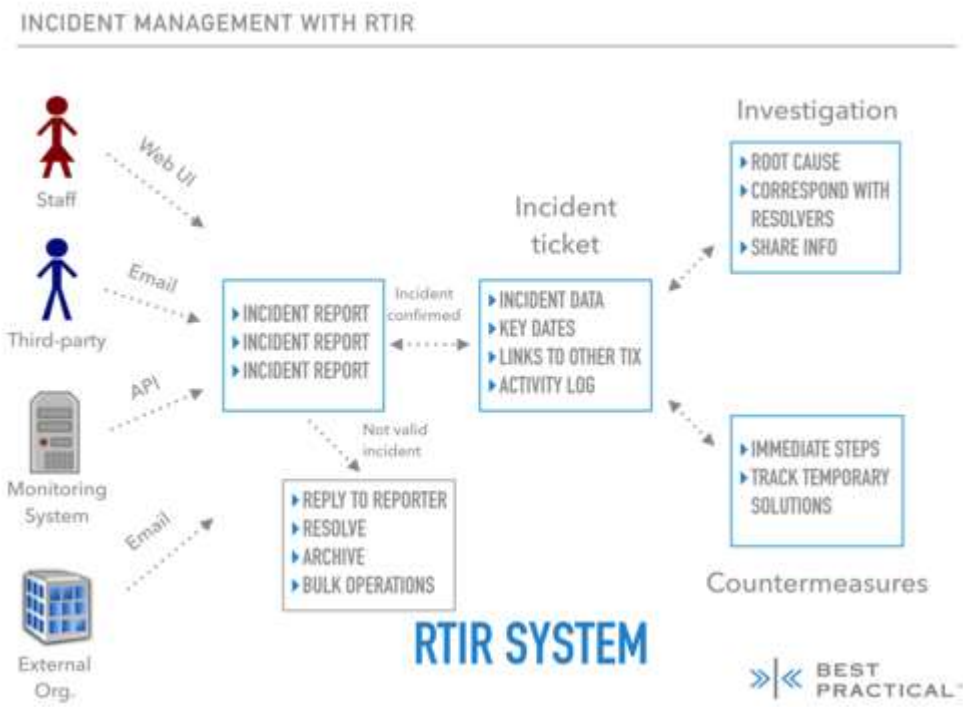


Main Incidents Management tool

- RT and RTIR ticketing system installed and configured in 2007.

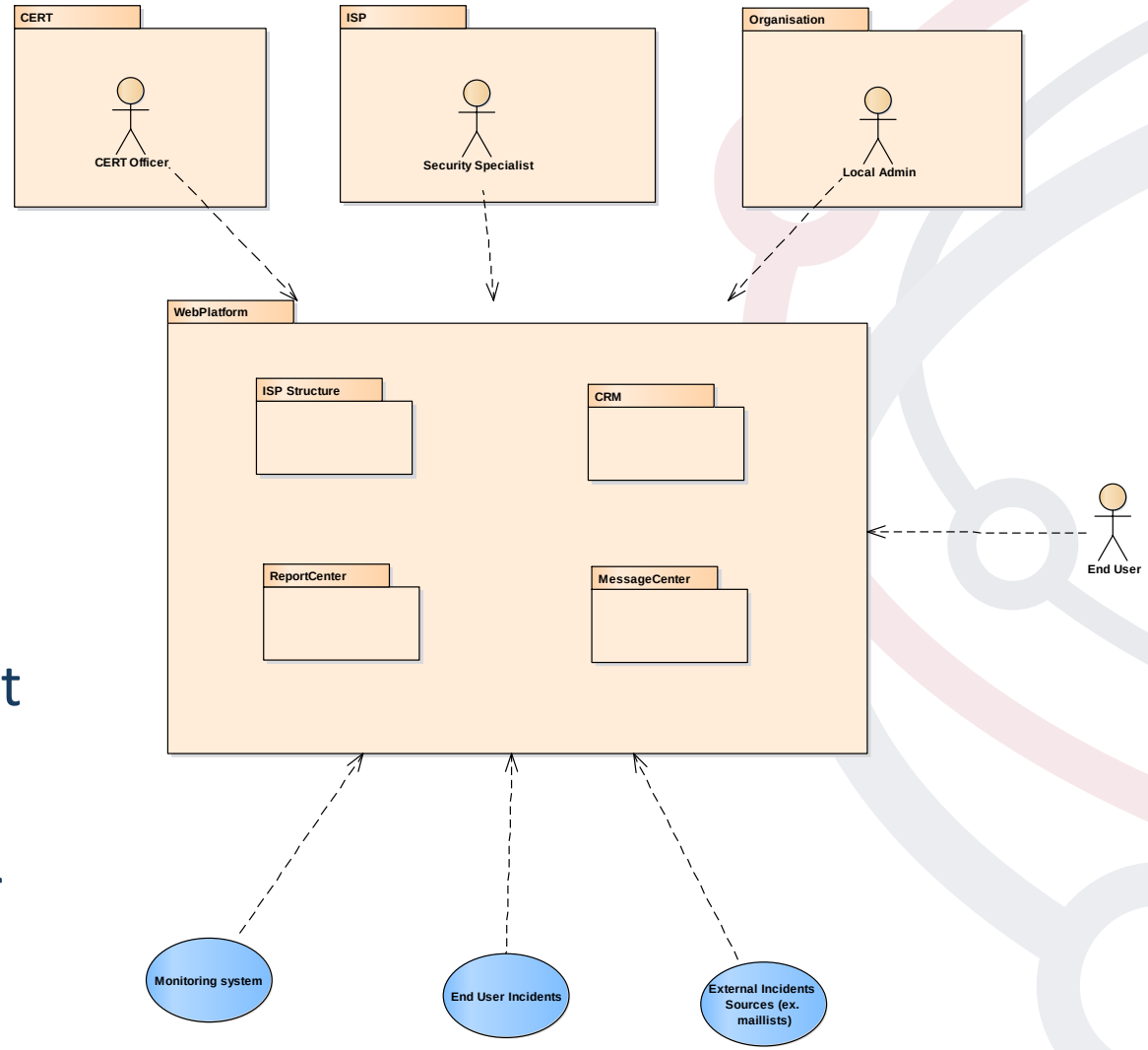
- Source:

  https://bestpractical.com/rtir



Incidents Platform

- Possibility of exchange and discuss security incidents
- Detailed ISP structure – “from end user to ISP” and country level structure “from ISP to central”.
- Build knowledge base of incident handling.
- More opportunities for end user

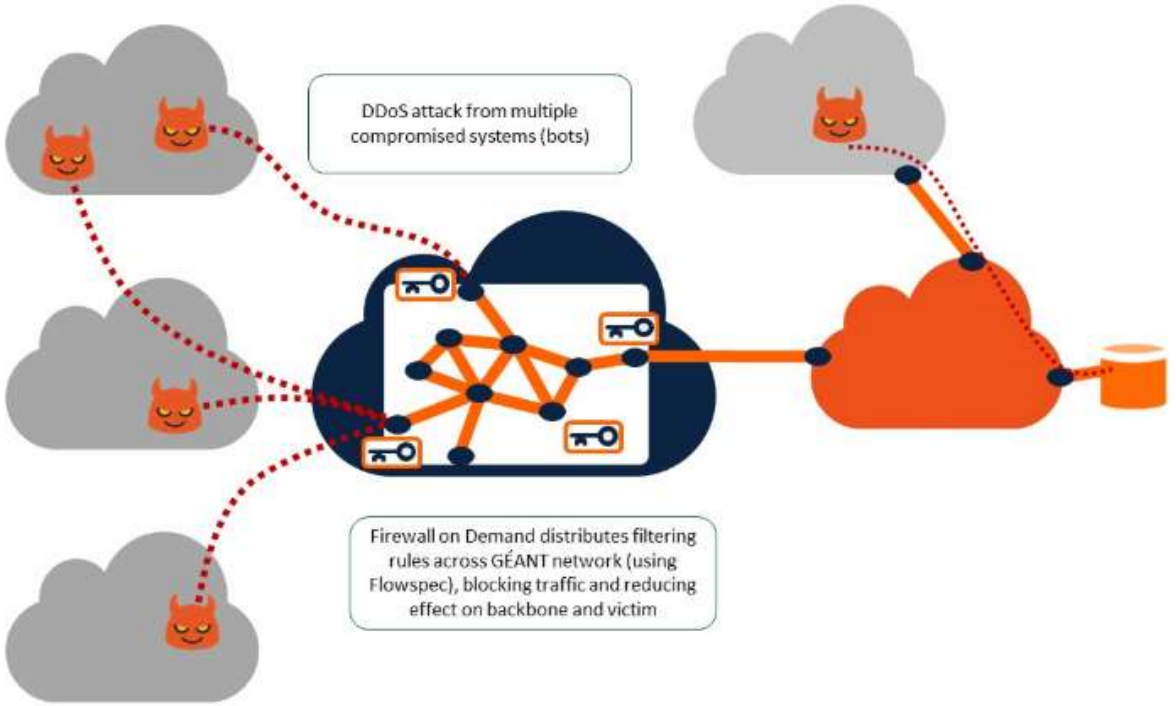


Crisis Management Exercise

- Identify how well organized the process of identifying and identifying an incident.
- Clearly define roles and responsibilities.
- Test critical thinking of employees.
- Check stress resistance.
- Check for backup options.
- Cooperation.
- Source: https://security.geant.org/claw-workshop/

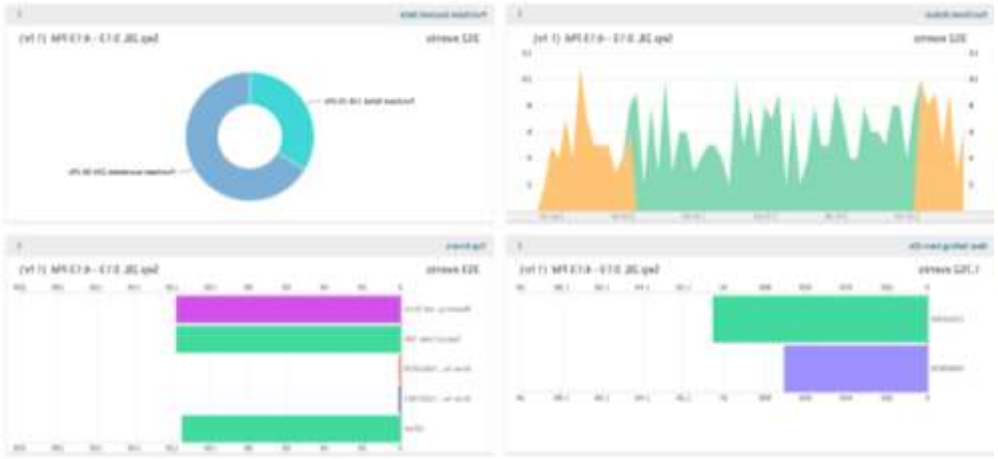
Firewall on Demand

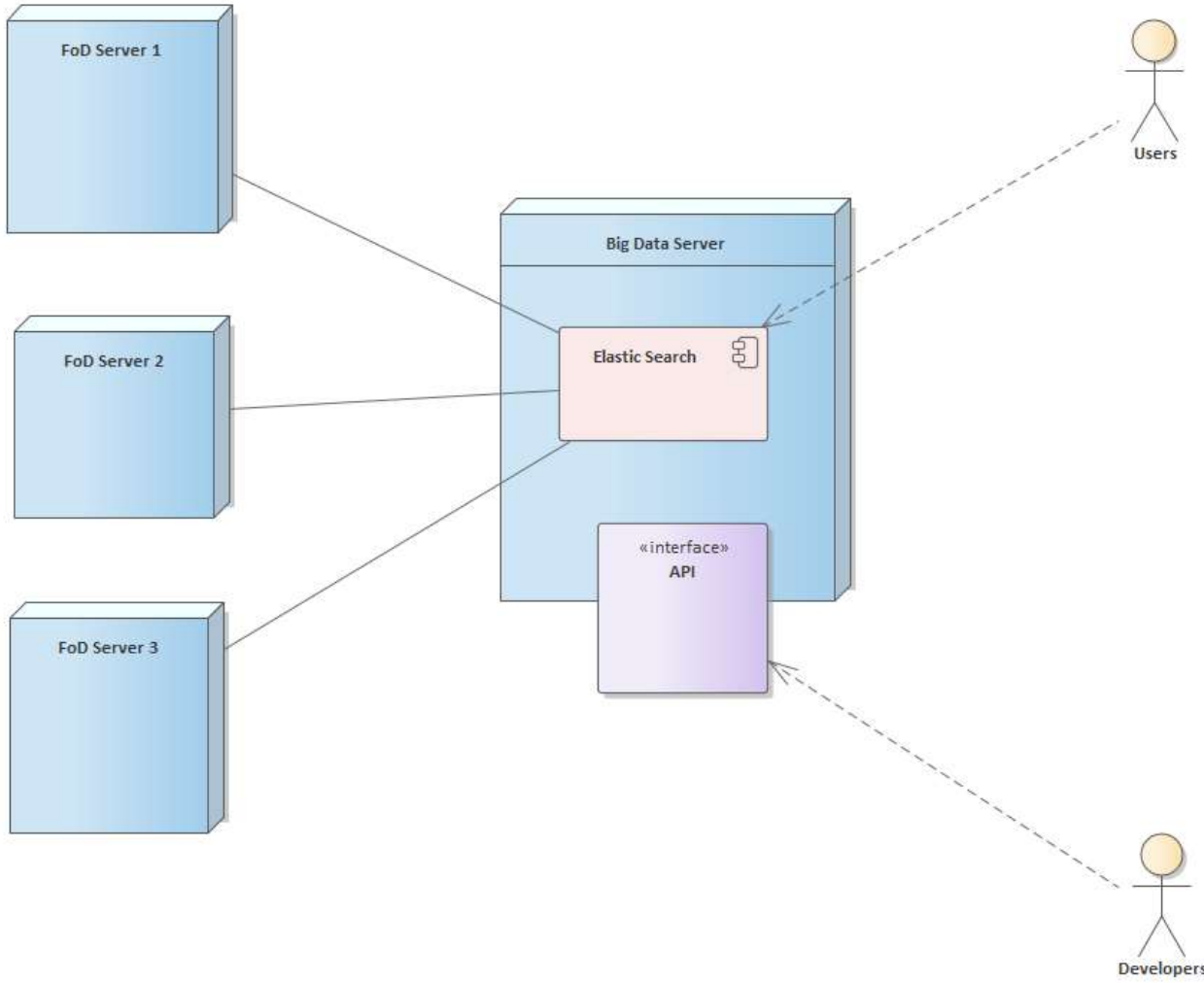
- Precision – specific malicious flows can be targeted
- Speed - Time to disseminate/withdraw firewall filters is sub 10 seconds
- Convenience - NREN users can use web portal themselves, or make request by phone or e-mail.
- Simplicity - The web portal uses intuitive, non-vendor specific GUI-based wizard to configure router firewall filters.
- Source: https://security.geant.org/firewall-on-demand/



FoD ElasticSearch

- Read Data from logs
- Process data by a background job
- Define a Dataset
- Data Enrichment
- Data Visualization





MD-CERT Contacts

Ecaterina Matenco - CERT Officer - ematenco@renam.md

Alexandr Golubev - Head of Cert Department - galex@renam.md

Sergiu Gaugas - Networking Specialist - sergiu.gaugas@renam.md

Mail for incidents – inc@cert.md

RENAM
RESEARCH & EDUCATIONAL NETWORKING ASSOCIATION OF MOLDOVA

Thank you!

Any questions?

RENAM, Chisinau, Moldova

Website: www.renam.md
Social media: @RENAM.MD @RENAM_AO