CERT/CC

Mongolian Cyber Emergency Response Team / Coordination Center

HISTORY

ESTABLISHED IN 2014 AS SECURITY COMMUNITY MEETUP

Transformed as non-governmental, non-profit organization in 2015

MISSION

Improve the technical capabilities of constituents

Provide support during incident response and threat intelligence activities

Establish the professional trust community for cyber security related information sharing and collaboration.

Raise the security awareness of the general public

Cyber drill

Training

Information sharing

Public awareness

Collaborate

MN CERT/CC

Mongolian Cyber Emergency Response Team / Coordination Center

INTERNATIONAL RELATION

COLLABORATION

ХАРИЛЦАА ХОЛБООНЫ ЗОХИЦУУЛАХ ХОРОО

DCERT
DATACENTER EMERGENCY RESPONSE TEAM

ШУТИС
МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ
МЭДЭЭЛЭЛ, ХОЛБООНЫ ТЕХНОЛОГИЙН СУРГУУЛЬ

НМТГ

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ГАЗАР

MEMBERS

Service Providers:

MobiCom

UNITEL

SKYtel

MONGOLIA NETCOM

NATIONWIDE BROADBAND NETWORK

Banking/Financial:

GOLOMT BANK

XACBANK

ТӨРИЙН БАНК

KHAN BANK

TDB

ХУДАЛДАА ХӨГЖЛИЙН БАНК

TransBank

ТЭЭВЭР ХӨГЖЛИЙН БАНК

Others:

ҮНЭТ ЦААСНЫ ТӨВЛӨРСӨН ХАДГАЛАМЖИЙН ТӨВ

itools

ЗОГСОЛТГҮЙ ХӨГЖИЛ, АМЖИЛТААРАА ЯЛГАРЪЯ

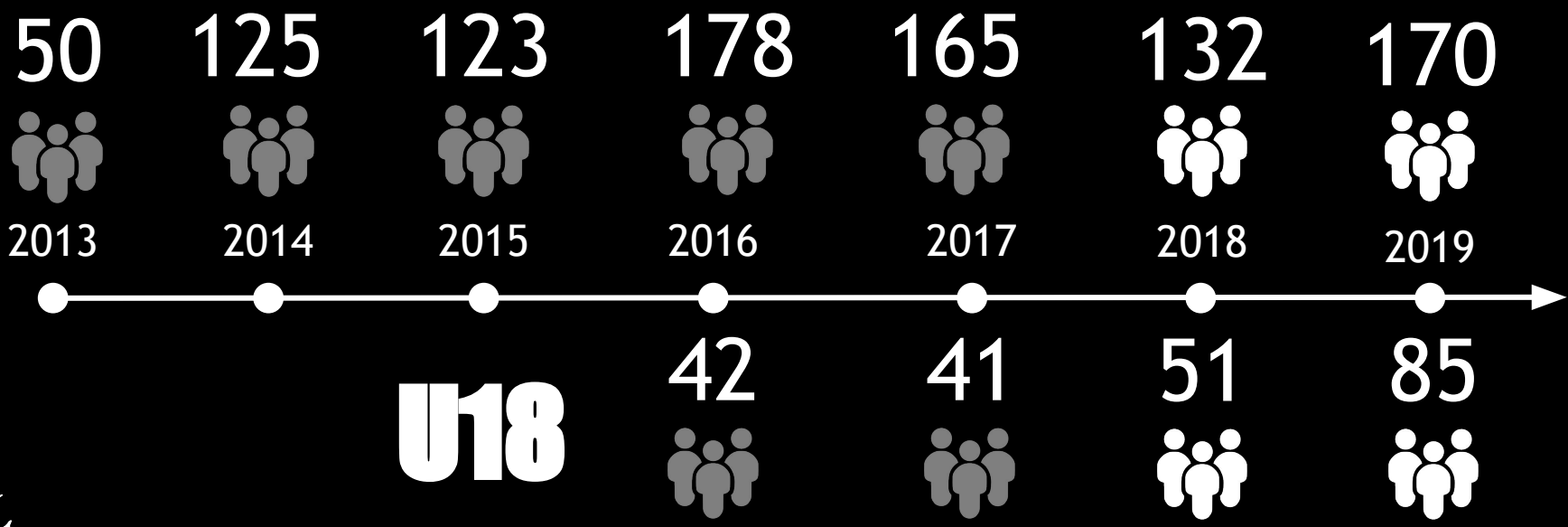
RioTinto

ORGANISED EVENTS

“Haruul Zangi” CTF

Since 2013

“Haruul Zangi” CTF Participants



INFO SECURITY CONFERENCE

Since 2014

MNSEC CONFERENCE

+1000

2014 2015 2016 2017 2018

CYBER DRILL

Since 2016

Cyber Security Training

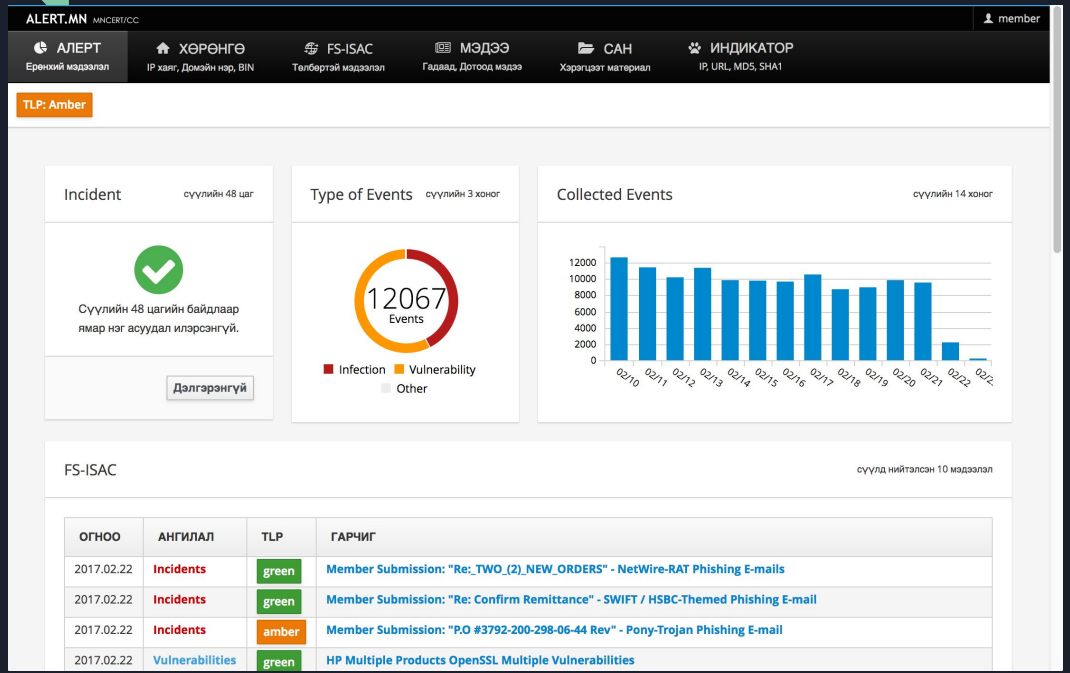
Since 2016

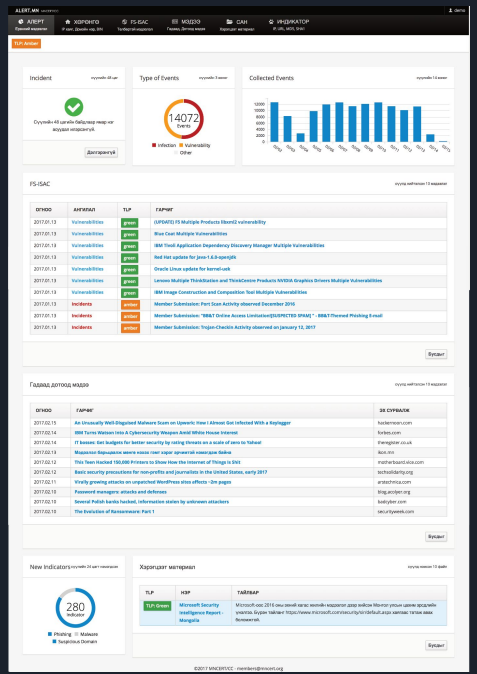
FIRST CSIRT training

CISSP training
MISP training

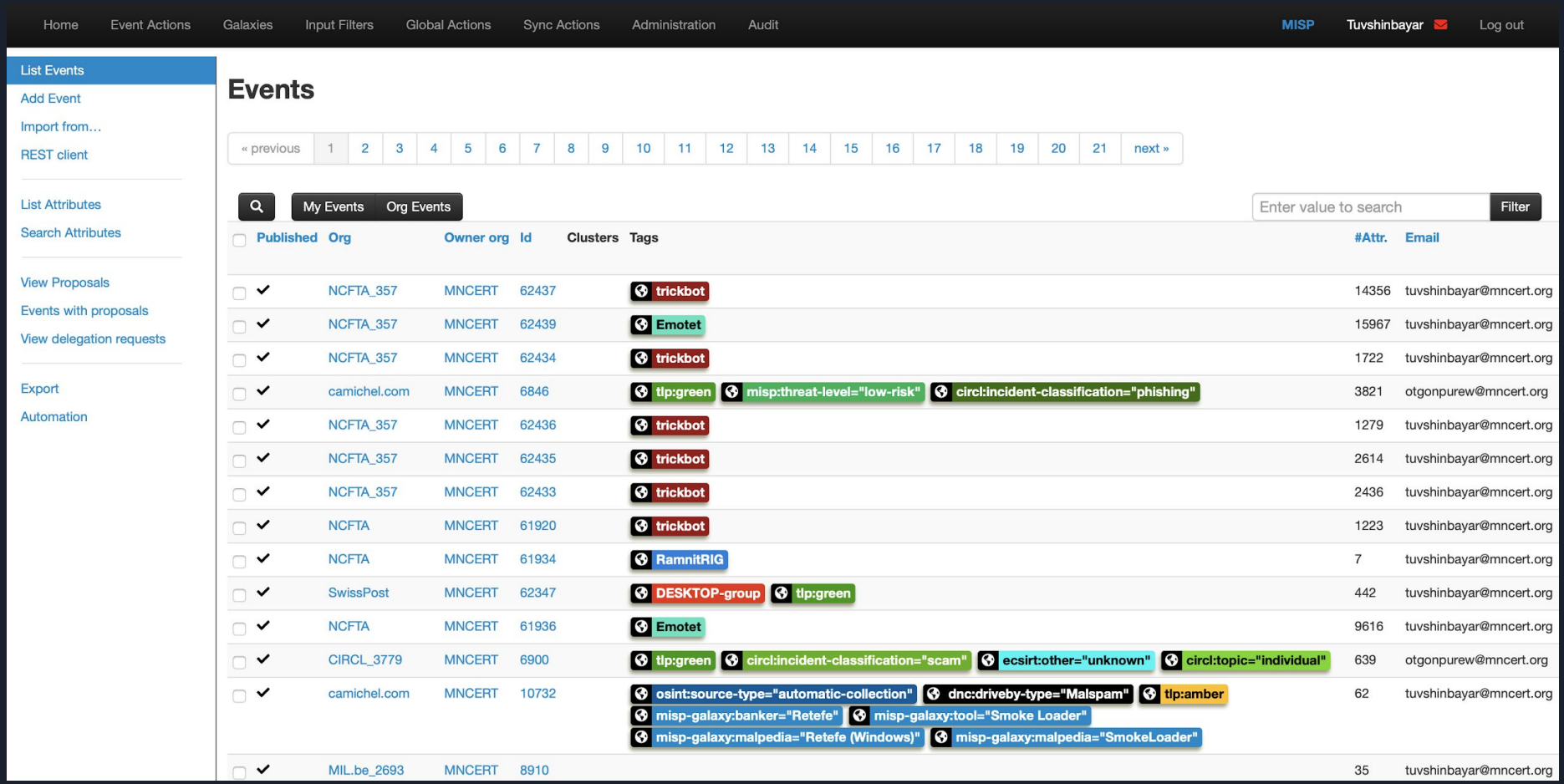
ACTIVE PROJECTS

ALERT.MH


ALERT.MN MNCERT/CC
member
АЛЕРТ
Ерөнхий мэдээлэл
ХӨРӨНГӨ
IP хаяг, Домэйн нэр, BIN
FS-ISAC
Төлбөртэй мэдээлэл
МЭДЭЭ
Гадаад, Дотоод мэдээ
САН
Харэгцээт материал
ИНДИКАТОР
IP, URL, MD5, SHA1
TLP: Amber
Incident
сүүлийн 48 цаг
Сүүлийн 48 цагийн байдлаар ямар нэг асуудал илэрсэнгүй.
Дэлгэрэнгүй
Type of Events
сүүлийн 3 хоног
12067
Events
Infection
Vulnerability
Other
Collected Events
сүүлийн 14 хоног
12000
10000
8000
6000
4000
2000
0
02/10
02/11
02/12
02/13
02/14
02/15
02/16
02/17
02/18
02/19
02/20
02/21
02/22
FS-ISAC
сүүлд нийтэлсэн 10 мэдээлэл
ОГНОО
АНГИЛАЛ
TLP
ГАРЧИГ
2017.02.22
Incidents
green
Member Submission: "Re:_TWO_(2)_NEW_ORDERS" - NetWire-RAT Phishing E-mails
2017.02.22
Incidents
green
Member Submission: "Re: Confirm Remittance" - SWIFT / HSBC-Themed Phishing E-mail
2017.02.22
Incidents
amber
Member Submission: "P.O #3792-200-298-06-44 Rev" - Pony-Trojan Phishing E-mail
2017.02.22
Vulnerabilities
green
HP Multiple Products OpenSSL Multiple Vulnerabilities



MISP.ALERT.MN



View Event
View Correlation Graph
View Event History

Edit Event
Delete Event
Add Attribute
Add Object
Add Attachment
Populate from...
Enrich Event
Merge attributes from...
Propose Attribute
Propose Attachment

Download as...

List Events
Add Event

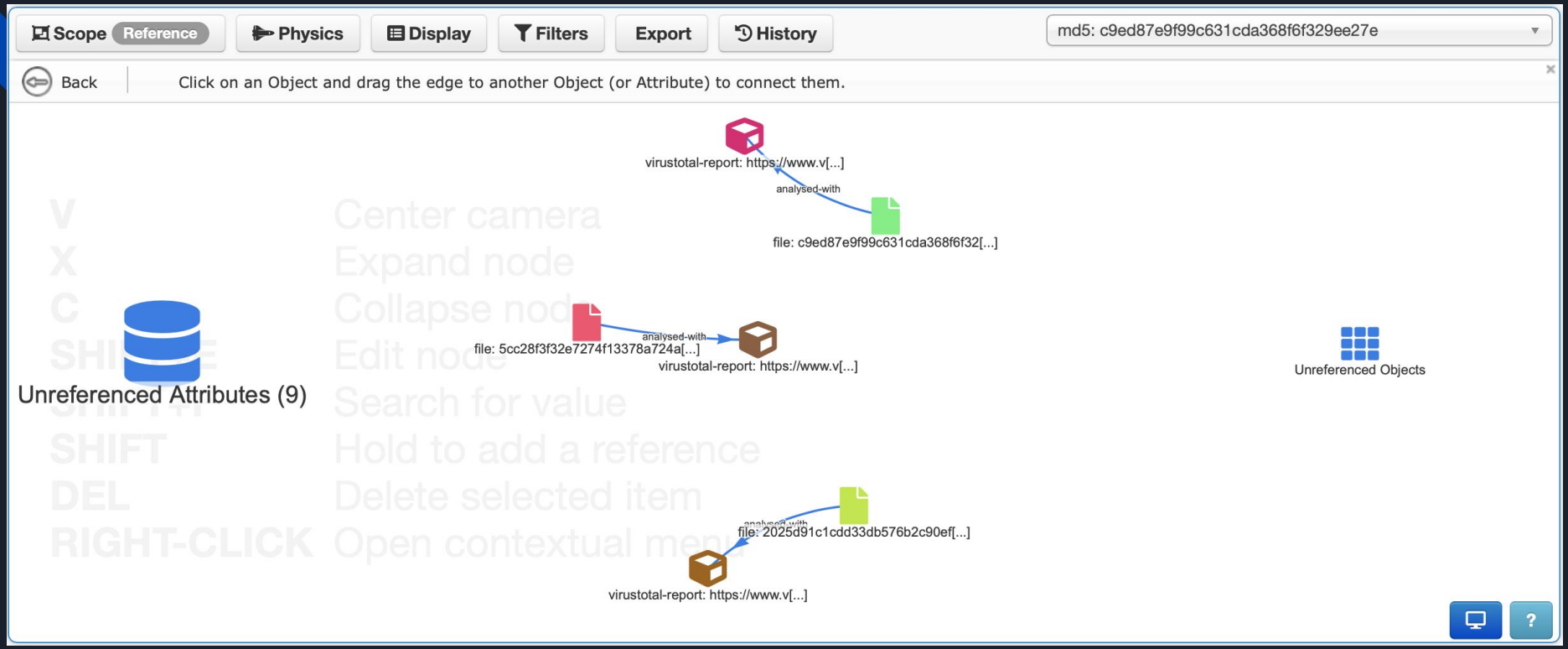
2019-01-25: Lazarus Pakistan Toolkits

Event ID	10092
UUID	5c4cb9a7-0454-42eb-8f63-383368f8e8cf
Creator org	VK-Intel
Owner org	MNCERT
Email	tuvshinbayar@mncert.org
Tags	Actor: Lazarus x, DPRK x, Malware: PowerRatankba,b x, PowerShell Installer x, Keylogger x, Country: Pakistan x, type:OSINT x, osint:lifetime="perpetual" x, osint:certainty="50" x, tlp:white x, misp-galaxy:threat-actor="Lazarus Group" x, misp-galaxy:malpedia="PowerRatankba" x, misp-galaxy:mitre-enterprise-attack-intrusion-set="Lazarus Group" x, misp-galaxy:malpedia="Lazarus" x, misp-galaxy:mitre-enterprise-attack-intrusion-set="Lazarus Group - G0032" x, misp-galaxy:mitre-intrusion-set="Lazarus Group" x, misp-galaxy:tool="PowerRatankba" x
Date	2019-01-26
Threat Level	Medium
Analysis	Initial
Distribution	All communities
Info	2019-01-25: Lazarus Pakistan Toolkits
Published	Yes (2019-09-26 02:02:05)
#Attributes	27 (6 Objects)
First recorded change	2019-01-27 10:50:55
Last change	2019-09-25 10:03:20

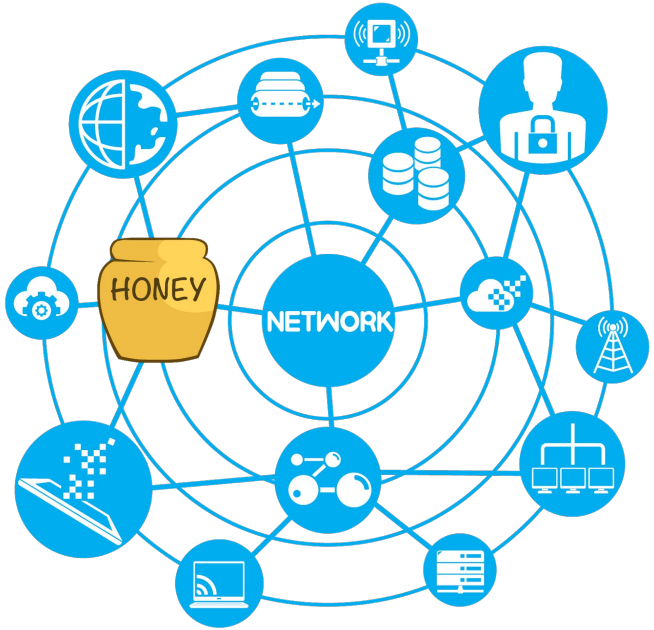
Related Events

Air... Lazarus PowerRatankba.B toolkit
Cy... *2019-01-28* **9**

Air... Lazarus DPRK Malware Sample
Cy... *2019-01-25* **3**


Scope
Reference
Physics
Display
Filters
Export
History
md5: c9ed87e9f99c631cda368f6f329ee27e
Back
Click on an Object and drag the edge to another Object (or Attribute) to connect them.
virustotal-report: https://www.v[...]
analysed-with
file: c9ed87e9f99c631cda368f6f32[...]
V Center camera
X Expand node
C Collapse node
SHIFT+E Edit node
SHIFT+F Search for value
SHIFT Hold to add a reference
DEL Delete selected item
RIGHT-CLICK Open contextual menu
Unreferenced Attributes (9)
file: 5cc28f3f32e7274f13378a724a[...]
analysed-with
virustotal-report: https://www.v[...]
Unreferenced Objects
file: 2025d91c1cdd33db576b2c90ef[...]
virustotal-report: https://www.v[...]

HONEYPOT



MEMBERSHIP

MN
CERT/CC
Mongolian Cyber Emergency Response Team / Coordination Center

Information sharing

- Local and international threat sharing, warning, vulnerability disclosures within member organizations.

- Fast, responsible and professional.

Trainings and Meet-ups

- Information security trainings
- Security experts monthly meet-ups and experience sharing

Professional Services

- Cyber drill workshops (onsite & webex)
- Incident Response (MNCERT members and worldwide)
- International conferences and event participation

CERT/CC

Mongolian Cyber Emergency Response Team / Coordination Center