CYBER SECURITY CENTER

BUILDING GOVERNMENT CYBERSECURITY WORKFORCE CAPACITY

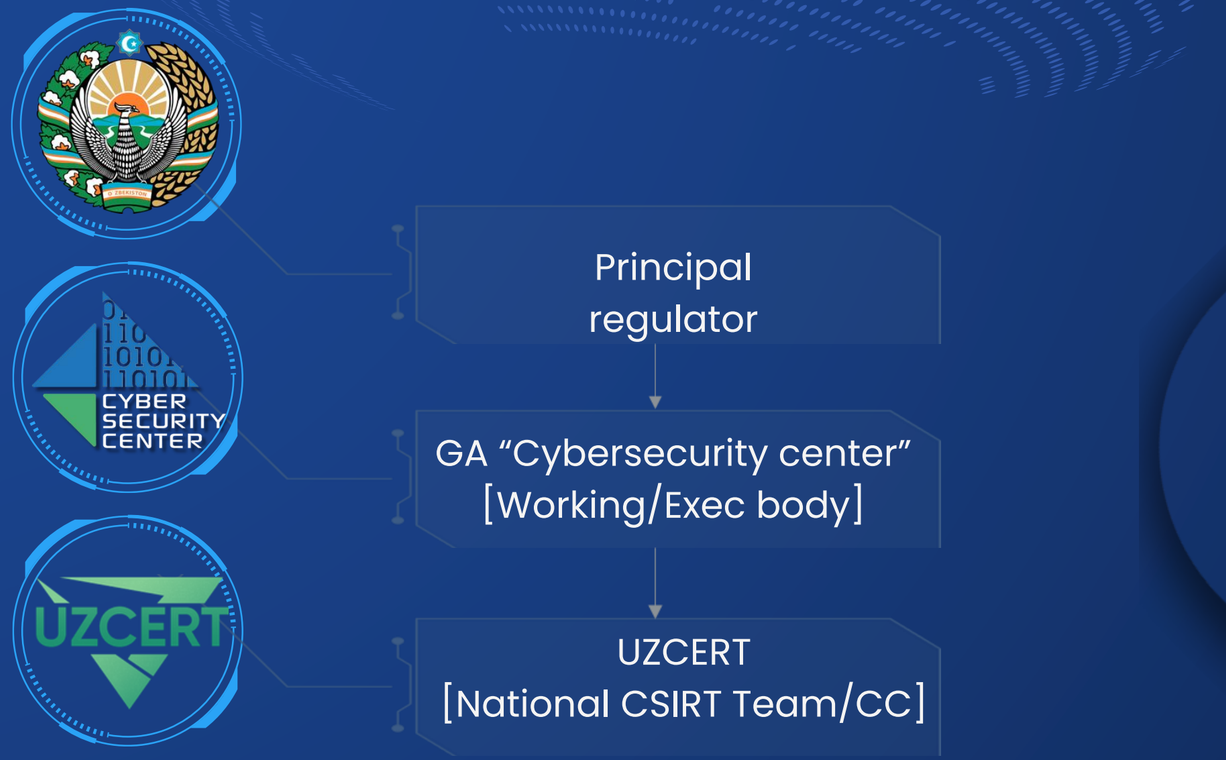
UZCERT's Experience and Best Practices

Azamat Abdullayev
GA "Cybersecurity center"
Republic of Uzbekistan

www.csec.uz
www.uzcert.uz

info@csec.uz
info@uzcert.uz

CYBERSECURITY IN UZBEKISTAN



🎯 Legal framework:

- Law of the Republic of Uzbekistan “On Cybersecurity” (LRU-764) (2022)
- “On Additional Measures for Ensuring Cybersecurity of Critical Information Infrastructure” (2023)
- “On Classification & Registry of Critical Information Infrastructure Objects” (2024)
- Presidential Resolution (PP-4452) “on measures for improvement of information security” (2019)

ABOUT US

- UZCERT - National Cyber Incident Response Team of Uzbekistan operating under “Cybersecurity center”
- Coordinating cyber incident response across government & critical sectors
- Incident handling, advisories, vulnerability notifications
- Capacity-building: training gov & CI teams, cyber exercises, CTF programs
- International cooperation with CERT/organizations, Exchange of threat intelligence and Indicators of Compromise (IOCs) with other CERT teams
- Full members at:

CHALLENGES FACED

- New cybersecurity & CII regulations expanded responsibilities nationwide
- Need to rapidly upskill 1,000+ cybersecurity staff across 200+ public organizations
- Limited resources in some small public organizations
- Fast-evolving threat landscape requiring continuous learning
- For the last 5 years cybercrime multiplied x68 times and damage exceeded $100m

ITU defines Capacity Building as one of five strategic pillars for national cyber-resilience. (Global Cybersecurity Agenda, ITU-D)

OUR APPROACH TO BUILDING CYBER CAPACITY

- Pure training & webinars ≠ real readiness
- Need for hands-on engagement, continuous practice, community
- Ecosystem approach
- Build skills through doing, not only listening
- Create pipelines, not one-time events
- Continuous Upskilling & Maturity

From knowledge to capability — from capability to resilience.

KEY PILLARS & ENGAGEMENT INITIATIVES

National engagement	•Stakeholder engagement across GOV, CII, Academia, Private sector •Support for sectorial CSIRTs
Hands-on skill development	•Cyber drills, Real life defense scenarios •Tabletop exercises, CTFs
Learning from real threats	•Early-warning system (EWS) •Real alerts, Malware & threat exchange (MISP)
Academic Talent Pipeline	•Cybersecurity programs across HEIs •Cybersecurity clubs, Communities
Continuous Maturity	•NICE role mapping, SIM3 maturity targets •Ongoing upskilling, Playbooks

PROJECT SPOTLIGHT: EARLY-WARNING (EWS)

- Moves defenders from training exercises → real-world threat handling
- Daily exposure to live threat data builds analyst muscle memory
- Reduces skill gaps by giving guided, actionable alerts
- Improves situational awareness, discipline & cyber hygiene
- Creates habit of continuous monitoring, response & improvement
- Builds confidence, readiness & maturity across the workforce

Don’t just train people – create an environment where defenders learn from real threats every day.

Source: https://www.arcticsecurity.com/resources/how-do-early-warning-systems-improve-cyber-and-it-effectiveness

PROJECT SPOTLIGHT: DRILLS, CTFS, EXERCISES

- Strengthens confidence, speed, and teamwork in critical moments
- Cyber drills for CII entities & Real-world scenario simulations
- CTFs among universities & public sector organizations
- Teams participating in international cyber battles such as Standoff365, KazHackStan

PROJECT SPOTLIGHT: NATIONAL BLUE-TEAM COMPETITION

- “CYBERKENT” - national “Blue Team” cyber battle
- Organized every year during “Cyber Security Summit – Central Eurasia (CSS)”
- Meeting point for Private & Public sector and Academia
- More than 95 “Blue Teams” and 290+ participants in 2025

GOVERNMENT-WIDE CYBER CAPACITY DEVELOPMENT

- “Cybersecurity Clubs” (now totalling 5 across Uzbekistan) to engage students and young professionals
- Establishment of the “Cyber University” of Uzbekistan offering specialist degree programs in cybersecurity & information security
- Expansion of cybersecurity education at universities: 20+ cybersecurity programs across HEIs & opening of cybersecurity labs
- Industry-academy partnerships delivering globally recognised certifications (e.g., partnership between EC-Council and Inha University in Tashkent) to build certified talent pool
- Cyber-Park initiative: incubating startups, hands-on learning, cyber entrepreneurship

CYBER SECURITY CENTER

UZCERT

THANKS FOR THE ATTENTION!

Azamat Abdullayev
GA “Cybersecurity center”
Republic of Uzbekistan

www.csec.uz
www.uzcert.uz

info@csec.uz
info@uzcert.uz