ISOC KAZAKHSTAN AND CYBERSECURITY CHALLENGE

Third Central Asian Internet Governance Forum

Astana 21-22 June 2018

Cybersecurity jobs are growing THREE TIMES FASTER than IT jobs in general.

There will be a global shortage of 2 MILLION cybersecurity professionals by 2019.

53% of employers currently take longer than SIX MONTHS to find qualified cybersecurity professionals.

84% of organizations believe that 50% or fewer applicants for open security jobs are qualified.

Source: ISACA Cybersecurity Skills Gap 2016, US Information Systems Audit and Controls Association

Networking Academy

https://cybersecurity.isaca.org

Information Systems Audit and Control Association

2016 Cybersecurity Skills Gap

Too Many Threats

$1 BILLION: PERSONALLY IDENTIFIABLE INFORMATION (PII) **RECORDS STOLEN IN 2014**[1]

97% BELIEVE APTs REPRESENT CREDIBLE THREAT TO **NATIONAL SECURITY AND ECONOMIC STABILITY**[2]

MORE THAN 1 IN 4 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[3]

$150 MILLION: AVERAGE COST OF A **DATA BREACH BY 2020**[4]

1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S **INTERNET OF THINGS (IOT) DEVICES**[5]

74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING **HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM**[6]

Too Few Professionals

2 MILLION: GLOBAL SHORTAGE OF CYBERSECURITY **PROFESSIONALS BY 2019**[7]

3X **RATE OF CYBERSECURITY JOB GROWTH** VS. IT JOBS OVERALL, 2010-14[8]

84% ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR **OPEN SECURITY JOBS ARE QUALIFIED**[9]

53% OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS **6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES**[10]

77% OF WOMEN SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER. **FOR MEN, IT IS 67%.**[11]

89% OF U.S. CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO **HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.**[12**]

Cyberattacks are growing, but the talent pool of defenders is not keeping pace.

Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate for university students to CSXP, the first vendor-neutral, performance-based cybersecurity certification, CSX is attracting and enabling cybersecurity professionals at every stage of their careers.

2018 Annual Cybersecurity Report

Discover security insights, key findings and the latest threat intelligence

Cisco Cybersecurity Reports Key Findings:

#1 Hackers launched even more powerful and sophisticated attacks in 2017

#2 Hackers are getting even better at hiding their command and control activities and evading defenses

#3 Hackers are exploiting security gaps in upcoming technology, such as Cloud and IoT

https://www.cisco.com/c/en/us/products/security/security-reports.html

Top 5 cybersecurity facts, figures and statistics for 2018

- **1. Cyber crime damage costs to hit $6 trillion annually by 2021.**
- **Cybersecurity spending to exceed $1 trillion from 2017 to 2021.**
- **Cyber crime will more than triple the number of unfilled cybersecurity jobs, which is predicted to reach 3.5 million by 2021.**
- **Human attack surface to reach 6 billion people by 2022.**
- **Global ransomware damage costs are predicted to exceed $5 billion in 2017.**

https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

A CSIRT is a team of IT security experts whose main task is to respond to computer security incidents. It provides the necessary services to handle them and support their clients to recover from breaches. In order to mitigate risks and minimize the number of required responses, most CSIRTs also provide preventative and educational services for their clients. They issue advisories on vulnerabilities in the soft and hardware in use, and also inform the users about exploits and viruses taking advantage of these flaws. So the clients can quickly patch and update their systems.v

CSIRT EXAMPLES

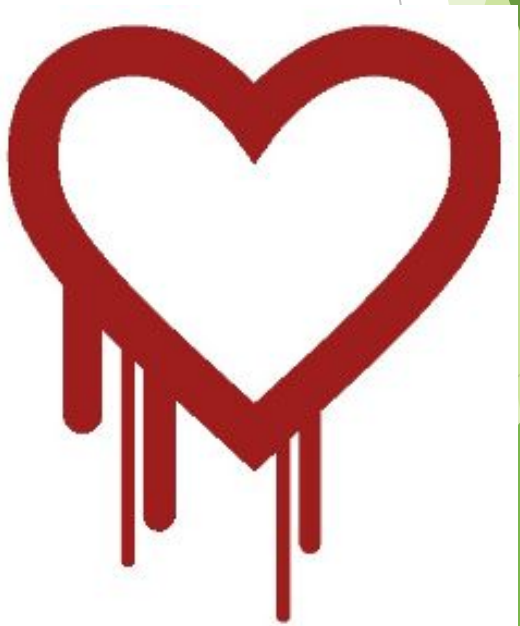
- Computer Security Incident Response Team
  - help ensure company, system, and data preservation by performing comprehensive investigations into computer security incidents
  - provides proactive threat assessment, mitigation planning, incident tre
    and security architecture review

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

APCERT
Asia Pacific Computer Emergency Response Team

FIRST
Improving Security Together

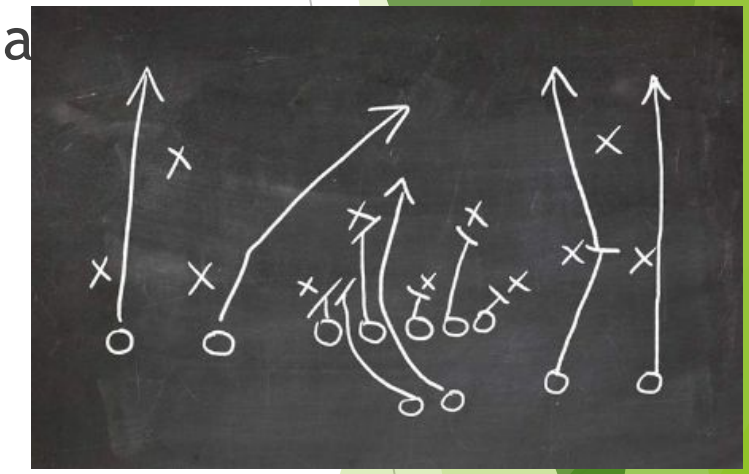
computer emergency response team | CERT-EU
for the EU institutions, bodies and agencies



Software Engineering Institute | Carnegie Mellon University

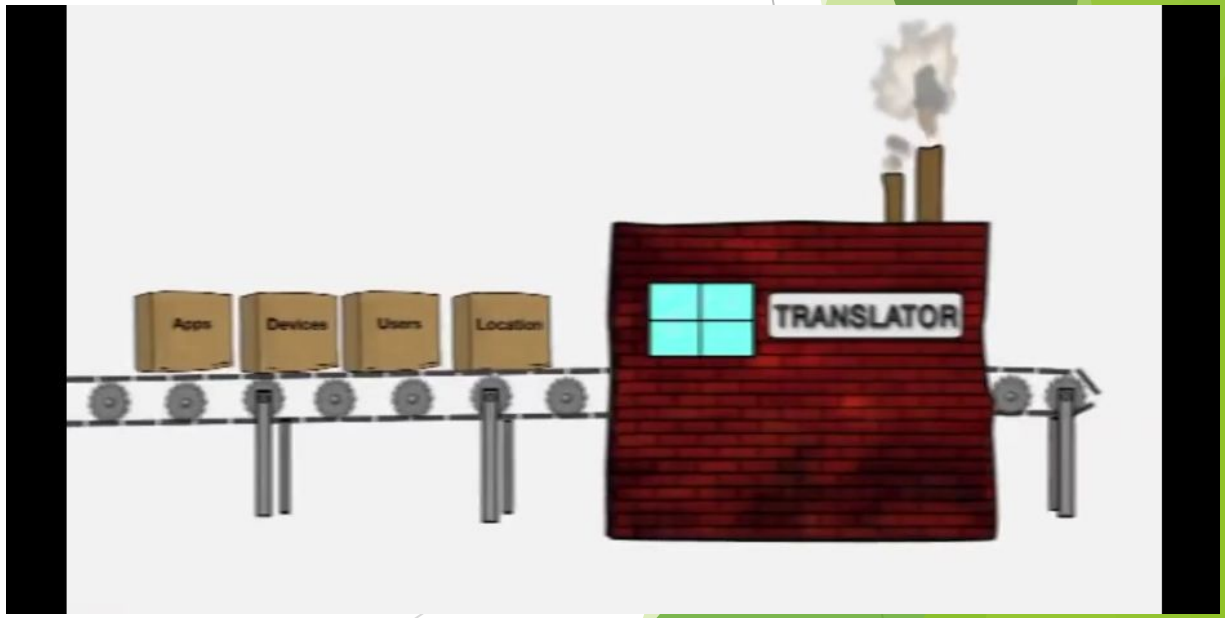
Security Playbook

- Collection of repeatable queries against security event da sources that lead to incident detection and response
- What does it need to accomplish?
  - Detect malware infected machines.
  - Detect suspicious network activity.
  - Detect irregular authentication attempts.
  - Describe and understand inbound and outbound traffic.
  - Provide summary information including trends, statistics, and counts.
  - Provide usable and quick access to statistics and metrics.
  - Correlate events across all relevant data sources.



Tools for Incident Prevention and Detection

- SIEM – Security Information and Event Management
  - Software that collects and analyzes security alerts, logs and other real time and historical data from security devices on the network
- DLP – Data Loss Prevention
  - Stops sensitive data from being stolen or escaped from the network
  - Designs to monitor and protect data in three different states



ISOC Kazakhstan Academic CSIRT project

The security of that systems and their availability in particular, is therefore of increasing concern to society.

Kazakhstan universities and academic institution are experiencing shortage or even absence of information security professionals which can provide protection of their digital infrastructure from various external and internal threats. The main goal of ISOC Kazakhstan - project is setting up Computer Security Incidents Response Team (CSIRT) for academic community in Kazakhstan.

ISOC Kazakhstan Academic CSIRT Activity

- 4 Training Workshops were conducted;
- More than 40 system administrators from 10 Kazakhstan Universities were trained;
- Security Onion SIEM was set up and providing monitoring security incidents monitoring in Kazakhstan Research and Educational Network (KazRENA);

GEANT TRANSITS-I Trainings 2017