Agenda

ABOUT

01

- ➢Organizational unit
- ➢Establishing
- ➢Constituents

SERVICES

02

- ➢Cybersecurity risk assessment
- ➢Email security standards and policies
- ➢Free Service WebCheck
- ➢Interactive Training Courses
- ➢Network Security Monitoring System
- ➢AntibotNet
- ➢MISP Threat Sharing Platform
- ➢Cyber-Responsible Organization
- ➢Awerness (Videos & Animations)
- ➢Automatic Malware Analysis

About

Organizational Unit

AEC

The National Centre for Computer Incidents Response (MKD-CIRT) is set up within the Agency for Electronic Communications as a separate organizational unit.

Establishing

2016

Established **2016**
The official national point of contact and for coordination in dealing with security incidents in networks and information systems.
Identifies and provides response to security incidents and risks.

Constituents

+130

All ministries, public administration and services of the Government.
Critical infrastructure operators in the Republic of N. Macedonia, and
Large organizations in the banking, transport, communication, health, energy and other strategic sectors in the country.

MKD-CIRT Services

Notifications and alerts

Disclose the details of current threats and steps that can be undertaken to protect against thes e threats. It includes notification or warning of newfound information on cyberthreats and vulner abilities to the constituents with a recommended course of action and guidance on how to prote ct the systems. The notifications may be preventive, warning, advisory, and guiding.

Remote incident response

Provide technical assistance to address the security incidents when they occur, in order to mitigat e the damage and recover from the incident. Advice and technical assistance is usually provided by telephone or e-mail..

On-site incident response

Provide on-site technical assistance and advice to address the security incidents when they occur, in order to mitigate the damage and recover from the incident. This service is usually related or implem ented for critical level incidents..

Awareness, education and training

Implement small-scale programs for raising public aw areness. Conduct basic training on computer incident response and main cybersecurity best practices.

Vulnerability response

Assess the adequate measures necessary to respond to newly discovered vulnerabilities; assess their seriousness and impact, decide whether to issue warnings thereof or verify or further investigate their weight/impact. Overall, this approach applies to information on vulnerabilities that are publicly known.

MKD-CIRT Service 1

Cybersecurity risks - assessment

HELP MKD-CIRT provide a BitSight service to constituents to help them better understand their own cybersecurity risks and those of their third-party partners.

Cybersecurity Ratings - identify and prioritize

Continuous Monitoring - identify and respond

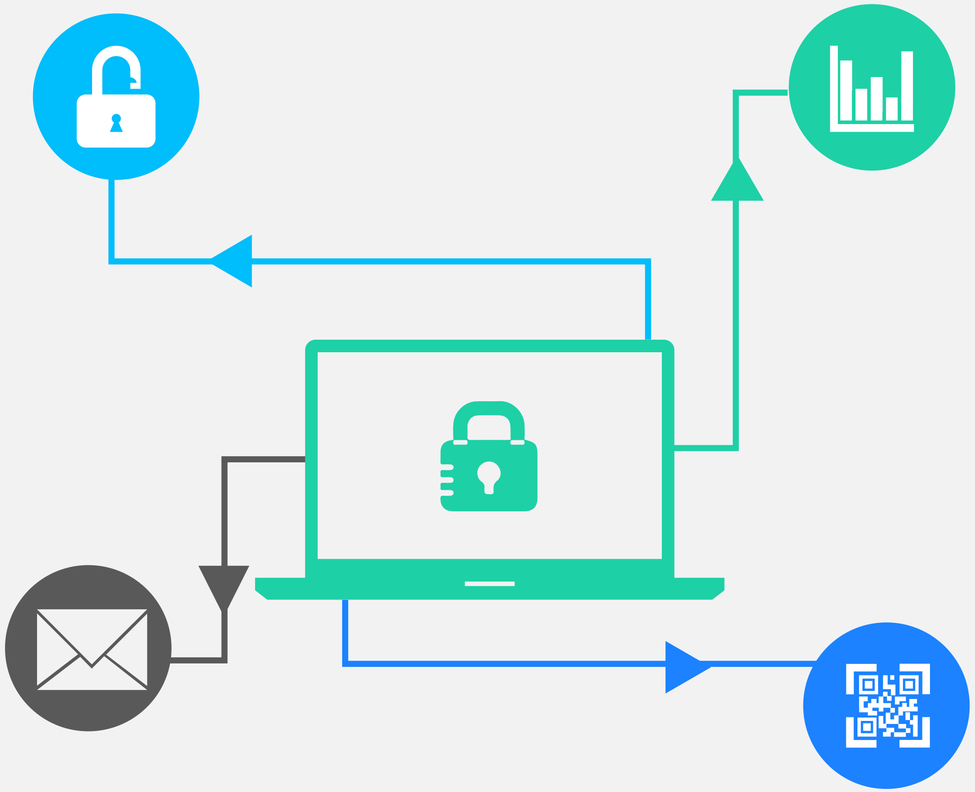
Third-Party Risk Management - identify and mitigate

Benchmarking – understand and improve

MKD-CIRT Service 2

Email security standards and policies

FREE PUBLIC SERVICE for new email security standards and policies
Generators & Validators
Analysis of reports



DKIM (DomainKeys Identified Mail)

email authentication protocol that allows organizations/companies to attach digital signatures to their email messages.

DMARC (Domain-based Message Authentication, Reporting & Conformance)

email authentication protocol that helps organizations/companies protect their email domains from spoofing and other types of email-based attacks.

SPF (Sender Policy Framework)

email authentication protocol that specifies which IP addresses are allowed to send email on behalf of a particular domain..

https://mailcheck.mkd-cirt.mk

MKD-CIRT Service 3

Free service **WEBCHECK**

WEBCHECK

WEB APPLICATION SCANING

Multitenant Model

- MKD-CIRT provides company level access
- Each organization can initiate discovery and vulnerability Scans
- Automated scanning and reporting

> “Better Visibility on vulnerabilities in public web sites for MKD-CIRT”

MKD-CIRT Service 4

Free Interactive Training Courses

Enrolled

+12000 citizens

11 cybersecurity topics each

Completed

+9000 citizens

2-hours long material

Certificate

upon successful completion of final quiz

Basic cyber security training

- public administration and private sector employees
- managerial staff in the public and private sector

Unique Certificate Code

Search by Certificate **ID**

by entering the code from the certificate, you can check the reliability and data of the training visitor.

MKD-CIRT Service 5

Network Security Monitoring System

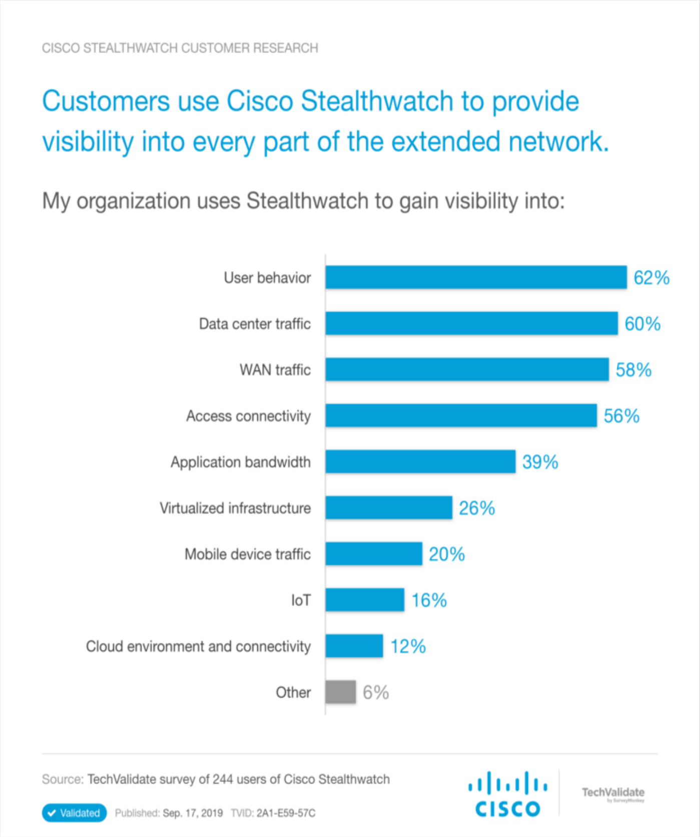
Cisco Stealthwatch

Network monitoring for
+10 organizations

Cisco Umbrella

+2500 end-point sensors

Systems for network and end-point monitoring, analysis and cyber security protection for the government and public sectors in North Macedonia



CISCO STEALTHWATCH CUSTOMER RESEARCH

Customers use Cisco Stealthwatch to provide visibility into every part of the extended network.

My organization uses Stealthwatch to gain visibility into:

Source: TechValidate survey of 244 users of Cisco Stealthwatch

✓ Validated Published: Sep. 17, 2019 TVID: 2A1-E59-57C

Anomaly detection using behavioral modeling

- Collect and analyze telemetry
- Create a baseline of normal behavior
- Alarm on anomalies and behavioral changes

Cloud-Based

- Prevention against phishing, malware, and ransomware attacks
- Visibility across all remote or on-site devices, ports, and cloud services
- Intelligence to uncover and defend against current and emerging threats

MKD-CIRT Service 6

ANTIBOTNET

MKD-CIRT's AntiBotNet service allows you to check whether your public IP address has been identified as a source of malicious activity that is a sign of possible compromise of the device or devices you access the Internet with.

List of Malicious Domains

potentially malicious and unknown domains

collected through the MKD-CIRT's Network Security Monitoring System

the list to block the specified domains on Firewall or other system

https://mkd-cirt.mk/antibotnet/

MKD-CIRT Service 7

MISP Threat Sharing Platform

MISP (Malware Information Sharing Platform) is an open-source platform designed to support the sharing of threat intelligence, particularly related to cybersecurity incidents and malware. Enables constituents to share and collaborate on indicators of compromise (IoCs), attack patterns, threat intelligence, and other security-related data.

Sharing and collaboration

MISP enables constituents to share and collaborate on threat intelligence, allowing them to stay up-to-date with the latest threat information.

Event management

MISP enables users to create, manage, and update events, which are collections of information related to a particular security incident or threat.

Customizable data models

The platform provides customizable data models, allowing organizations to define their own data structures for different types of information.

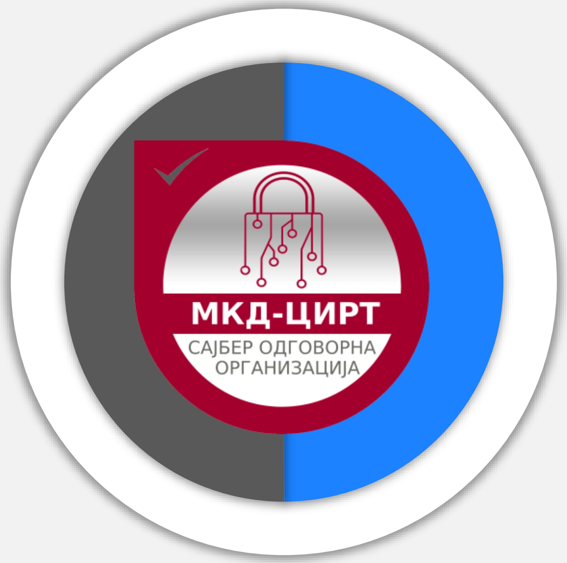
https://misp.mkd-cirt.mk

MKD-CIRT Service 8

Cyber-Responsible Organization

Self-assessments questionnaire
for certification scheme
‘Cyber-Responsible Organization’

MKD-CIRT issues a badge for recognition
Service is available free of charge at
https://mkd-cirt.mk



- **Safe business operations**
- **Secure configurations**
- **Upgrades and patching cadence**
- **Access control**
- **Viruses and malware**
- **Cyber Attacks and Incident Management**

https://mkd-cirt.mk/odgovorno-rabotenje-na-internet/

MKD-CIRT Service 9

Programs for raising public awareness

Video

and Animations

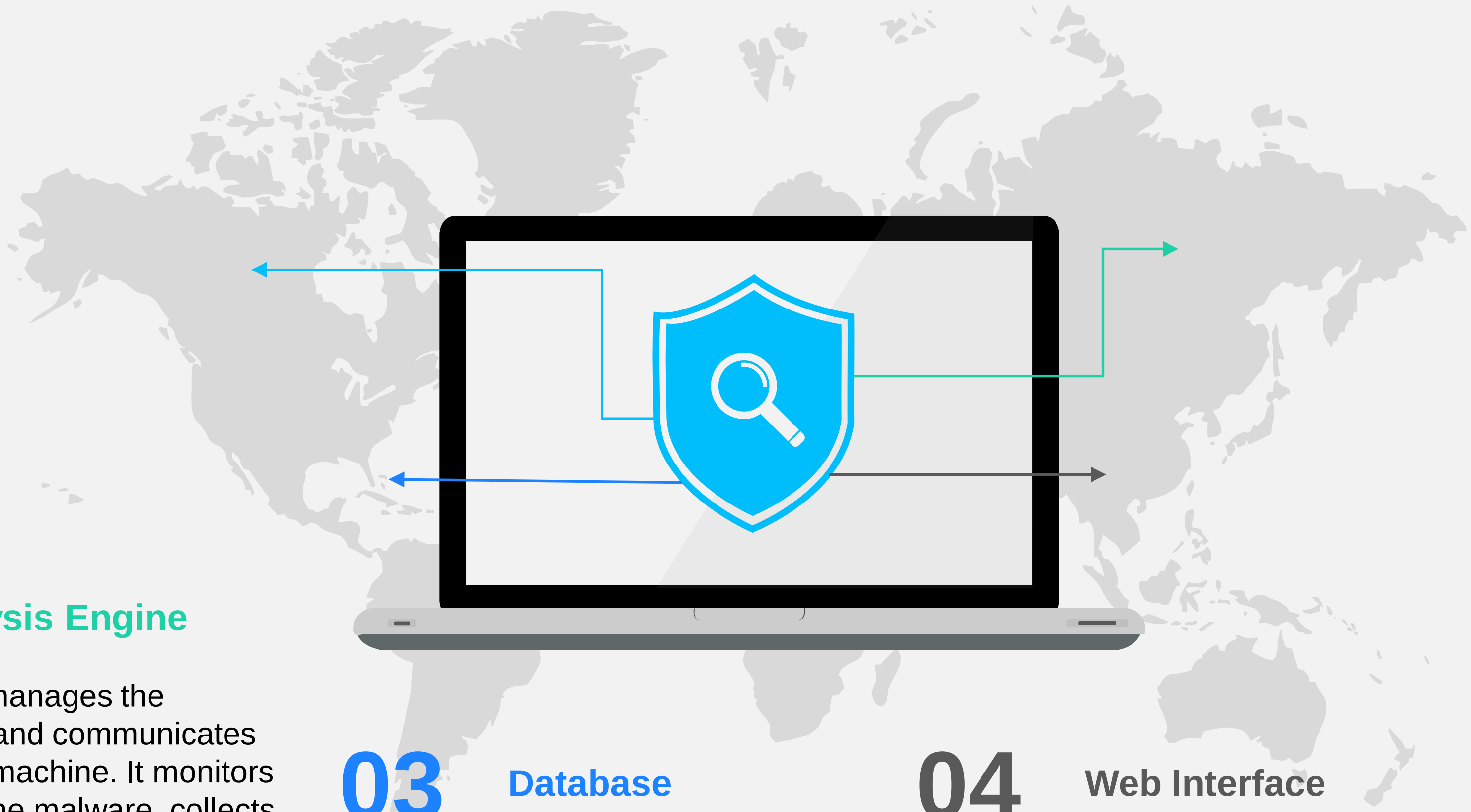
https://www.youtube.com/@mkd-cirtaec2681

MKD-CIRT Service 10

Automatic Malware Analysis

AMA

an open-source, community-driven malware analysis platform that provides a dynamic and configurable environment for malware analysis.



01 Analysis Machine

is the virtual machine where the malware is executed and observed. It can be configured with different operating systems, such as Windows or Linux, and different software configurations.

02 Analysis Engine

This component manages the analysis process and communicates with the analysis machine. It monitors the execution of the malware, collects data, and generates reports.

03 Database

Cuckoo stores the analysis results, metadata, and configuration data in a database for later reference..

04 Web Interface

The web interface provides a graphical user interface (GUI) for managing and monitoring the analysis process. It allows users to submit files for analysis, view reports.

https://ama.mkd-cirt.mk (accessible only from N.Macedonia)

THANK YOU FOR YOUR ATTENTION!

Sevdali Selmani

sevdali.selmani@aec.mk

National Center For Computer Incident Response **MKD-CIRT**
https://mkd-cirt.mk | contact@mkd-cirt.mk