# INTRODUCTION OF A NEW TEAM:

# ISTROCSIRT

HENRICH SLEZÁK

TLP: WHITE

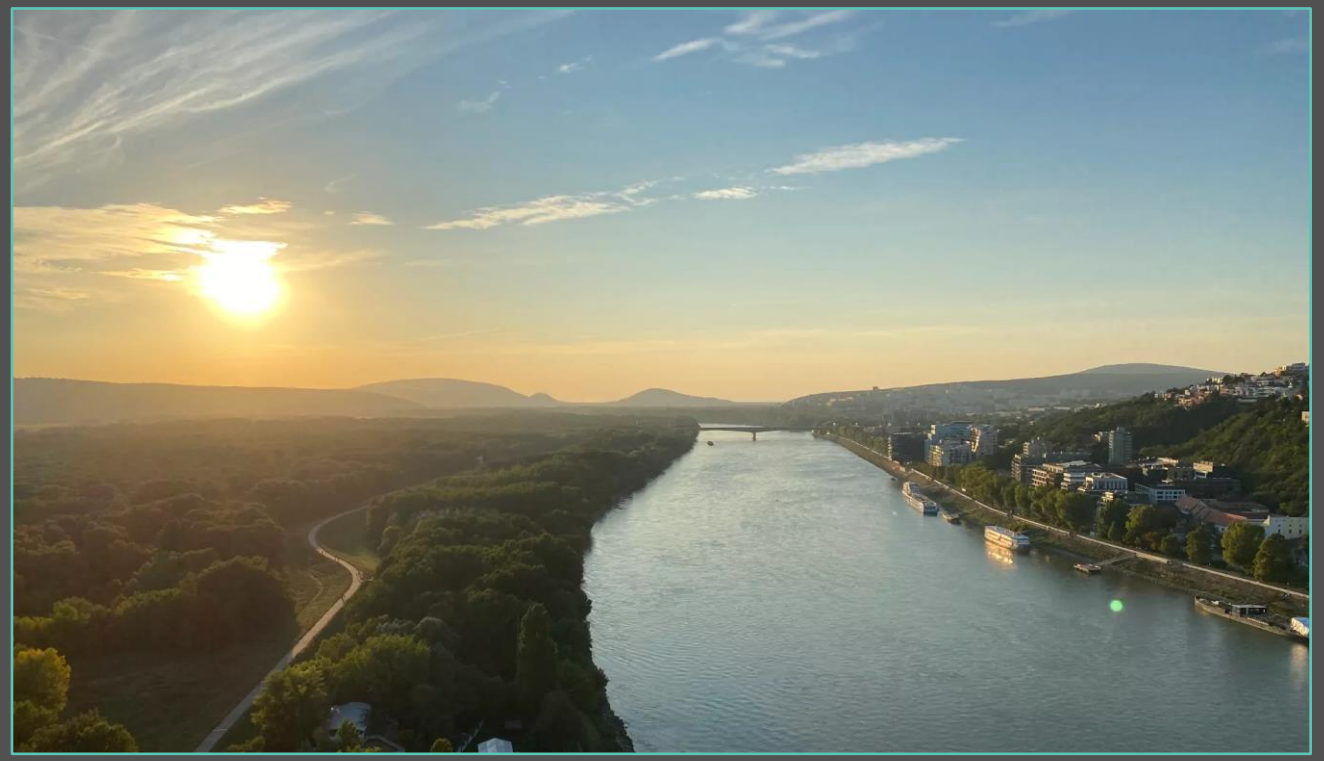
WWW.ISTROSEC.COM

IstroSec

3 MARCH 2022

# ISTROS

The ancient Greek name for the lower section of the Danube



# ISTROCSIRT LISTED IN TI



| | |
|---|---|
| **Official Name:** | IstroSec Computer Security Incident Response Team |
| **Short Name:** | IstroCSIRT |
| **Country:** | Slovakia |
| **Established:** | 01 Oct 2021 |
| **Host Organisation:** | IstroSec s.r.o. |
| **Constituency:** | Constituency of IstroCSIRT consists of institutions of any type, size or industry, which signed an agreement with the host company IstroSec s.r.o. as well as customer base of IstroSec s.r.o products. |

# ISTROCSIRT'S MISSION

ISTROSEC is an ethical company that conducts its business activities honestly, apolitically, directly and fairly to all parties involved.

### IstroSec's Vision

To be an international leader in research, development and cyber security services and deliver strong, innovative and effective solutions to tackle cybersecurity challenges.

### IstroSec's Objectives

Our goal is to offer quality professional services to our customers at a reasonable price and to continuously increase our customer's security resilience.

### IstroSec's Experiences

We have a track record of hundreds of incident response engagements, including APT groups, our own CVEs and countless pentests, malware analyses and trainings.

### IstroSec's Clients

Our customers are SMEs, corporations, Fortune 500 companies and governmental entities across all industries which take cyber security very seriously.

# OUR SERVICES

www.istrosec.com

### Incident Response

Rapid on-site deployment and remote response and mitigation of computer security incidents

### Digital Forensics

Acquisition of digital evidence, investigation, and reconstruction of security incidents

### Malware Analysis

Analysis of properties, functionality, origin and potential impacts of malicious code

### Threat Hunting

Active hunting for threats in infrastructure based on TTPs and searching for indicators of compromise

### CSIRT Services

Full array of CSIRT services, including 24/7 DFIR and proactive security

### Incident Preparedness

Assessment of adequacy of processes and technology for swift and effective reaction.

### Offensive Security

Vulnerability Assessment, Penetration Testing, Red Team and Purple Team Engagements

### Attack Simulations

Phishing, Spearphishing, Whaling. Custom Scenarios incl. Custom “Malware”

### Managed Defense

SOC Level 3 + Level 4. Network and Endpoints. EDR, SIEM, SOAR.

### Defensive Intelligence

Data Leaks Searches and Analysis, ClearWeb, DeepWeb, DarkWeb

### Advisory Services

Audits and Implementations of Security Frameworks, vCISO. Technical Audits and Hardening

### Trainings and Exercises

Trainings for personnel, IT professionals and management. Tabletop exercises and drills

# OUR TEAM

## ACHIEVEMENTS

- Found multiple vulnerabilities in operating systems, IT and OT systems (10 assigned CVEs, 15 more in process)
- Part of winning team of Locked Shields exercise (4 members of the team)
- Authors and co-authors of multiple research topics  presented in top conferences in the world (including DefCon, CyberCrimeCon, Black Hat, TF-CSIRT, etc.)
- Authors and co-authors of multiple cybersecurity tools (Gargamel, Ransomware vaccine, IOC checker, ESET Log parser, etc.)

## EXPERIENCE

- Incident response and cyber defense operations in governmental institutions, global financial, fintech, technology and non-profit organizations
- Performed more than 300 incident response, forensics engagements and cyber defense against 13 APT threat actors
- Penetration testing and red team engagements in Fortune 500 companies, governmental institutions, non-profit organizations
- Carried out  more than 240 red team and penetration test engagements

# OUR CERTIFICATES



# THANK YOU!

ANY QUESTIONS?

IstroSec

# CONTACT US



INFO@ISTROSEC.COM


+421 917 699 002


WWW.ISTROSEC.COM


WWW.ISTROSEC.COM/BLOG/


IstroSec