CTI és SOC újdonságok a Telekom biztonsági szolgáltatásaiban

Hlavaty Győző
Magyar Telekom
SOC vezető

Néhány érdekesség a hírszerzésről

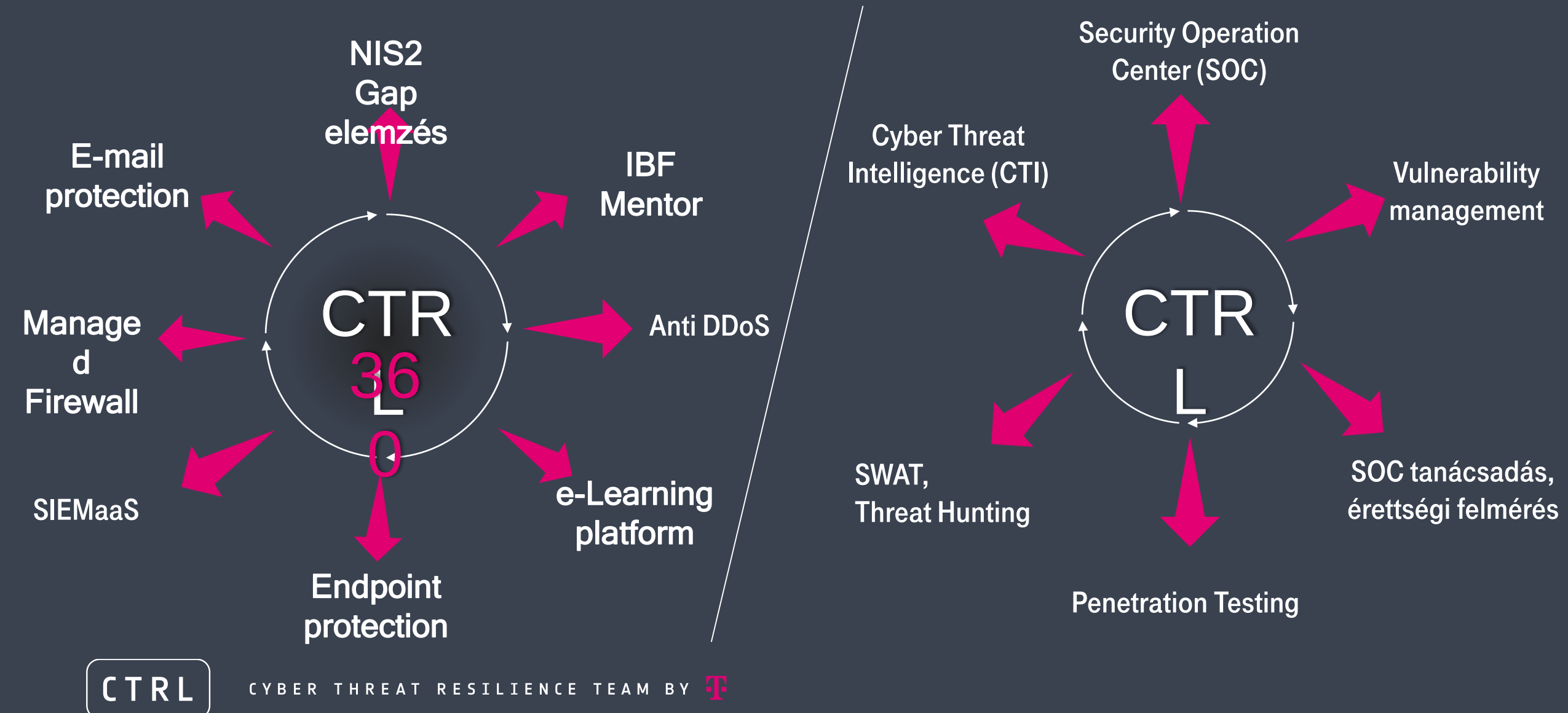
A tudásmegosztás mérföldkövei – a CTI alapjai

- Első Interneten terjedő vírus – 1988
- Első Internetszolgáltató – 1991
- Vírusok és malware-ek aranykora – 199x
- Freenet – 2000
- TOR Network – 2002
- STUXNET – 2010
- Lockheed Martin, SONY, RSA – 2011
- VIRUS-L mail list – 1988
- Első CERT/CSIRT – 1988
- National Vulnerability DB – 1999
- Abuse IP DB – 2002
- VirusTotal – 2004
- MALCON – 2010
- Cyber Killchain modell – 2011
- Recorded Future – 2012
- MITRE ATT&CK framework – 2013
- Mandiant – 2013

A Cyber Threat Intelligence piramis

Strategic	Vezetők és döntéshozók	Hosszú távú tervezés *Ki és miért?*
Tactical	Mérnökök és elemzők	Középtávú védekezés *Hogyan és hol?*
Operational	Elemzők és eszközök	Rövid távra összpontosít *Mivel?*

Telekom Managed Cybersecurity Services



CTRL CYBER THREAT RESILIENCE TEAM BY T

CTI – Gyártók, partnerek

Recorded Future®

MSSP partnerség

osint open source intelligence

Sodan, HackerTarget, Virustotal, HavelbeenPwned ...

Deutsche Telekom

Belső IOC-k és Brand monitoring

Fortinet FortiGuard, Trellix GTI

Trend Micro Threat Intelligence

...

cisco | Talos

cisco Umbrella

IBM X-Force

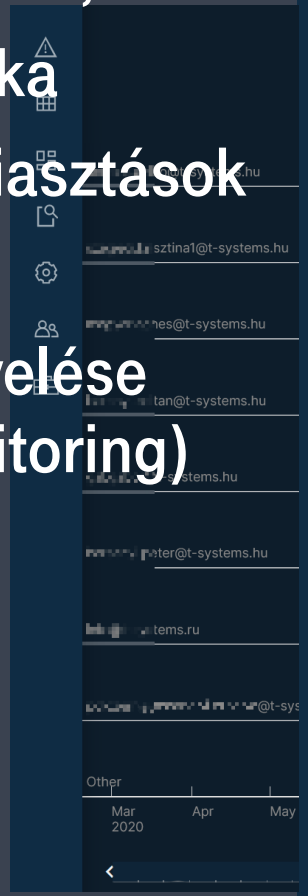
Kaspersky Threat Intelligence

CYBER INTEL MATRIX

MANDIANT

SOC használati eset

- Stratégiai információk, trendek
- Riporting, infografika
- Brand monitoring riasztások
- CTI alertek
- Beszállítói lánc figyelése (Supply Chain monitoring)



CTRL CYBER THREAT RESILIENCE

Magyar Telekom
Search
Ask AI

Recorded Future AI
New AI Conversation

GH

What types of vulnerabilities were exploited in the Wi-Fi routers targeted by hackers, and what brands were affected?

✓ Retrieving intelligence about **Cyber Attack**, **Cyber Vulnerability and Exploit**, **mesh Wi-Fi routers**, **Russian Hackers** for the time range **2024-10-28 to 2024-11-27**

Hackers exploited two critical vulnerabilities in Wi-Fi authentication protocols, specifically tracked as **CVE-2023-52160** and **CVE-2023-52161**. These vulnerabilities were found in the **wpa_supplicant** and **iNet Wireless Daemon (IWD)** software.[1] The flaws allowed threat actors to bypass authentication, which could enable them to intercept traffic on enterprise networks and gain unauthorized access to home Wi-Fi networks.[2]
Affected brands included major platforms that utilize these Wi-Fi authentication protocols, potentially impacting billions of users on devices running **Android**, **ChromeOS**, and **Linux**.[3] The report did not specify exact brand names but highlighted that many devices utilizing these protocols were vulnerable.[4] Users were advised to update their systems and follow recommended security practices to mitigate these risks.[5] 11:22 AM

Queried for Event Type: Cyber Attack, Cyber Vulnerability and Exploit Involving: mesh Wi-Fi routers, Russian Hackers
Event Time: 2024-10-28 to 2024-11-27

Follow-Up Questions

What critical vulnerabilities have been identified in Cinterion cellular modems and what sectors are at risk?

Which specific methods and infrastructures were utilized by the TAG-110 attacker group in their cyber operations?

What recent trends have been observed in cyberattacks against U.S. officials and defense contractors, particularly regarding Russian hacker groups?

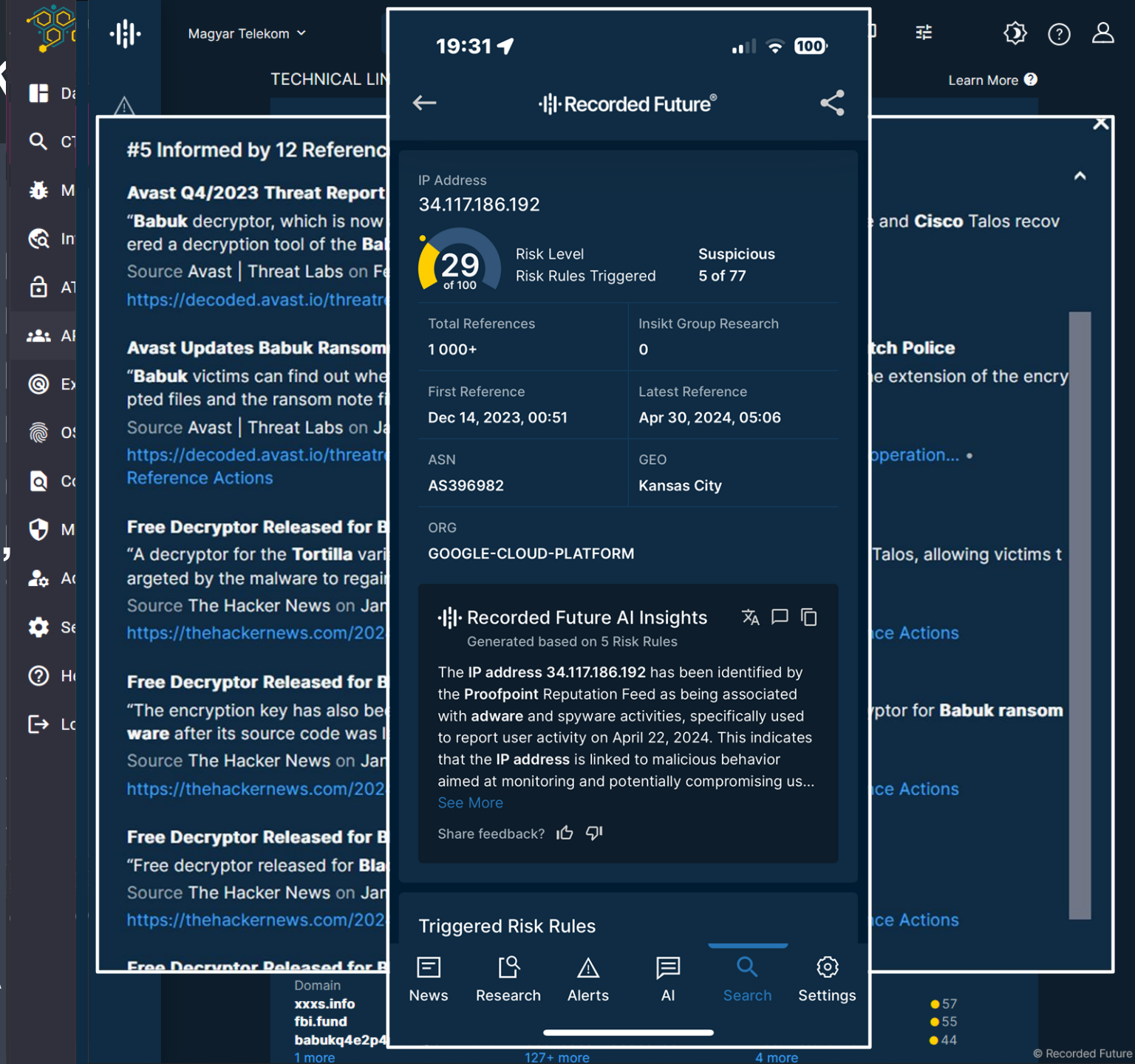
Ask Anything. Use Watch Lists - "my domains" or "/" shortcut.

SOC használati esetek

- Leaked credentials
- IP és Domain információk (Forensics)
- APT csoportok és jellemzőik
- Technikai információk (CVE, IOC, TTP...)

- Hasznos hivatkozások
- ...bárhol, bármikor

CTRL CYBER THREAT RESILIENCE TEA



Hlavaty Győző
SOC vezető
hlavaty.gyozo@telekom.hu

CTRL SWAT 7/24 Hotline: +36 1 481 9911