

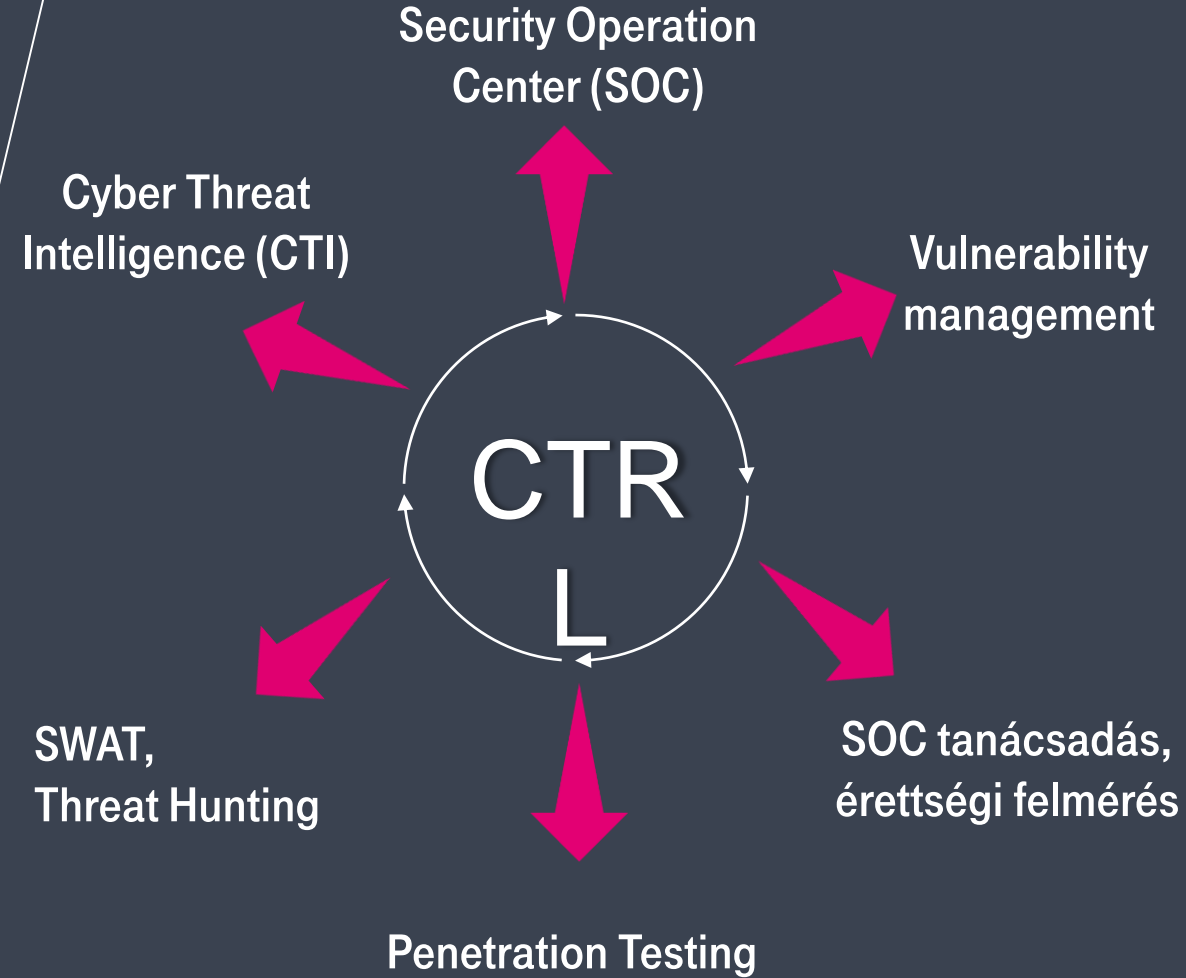
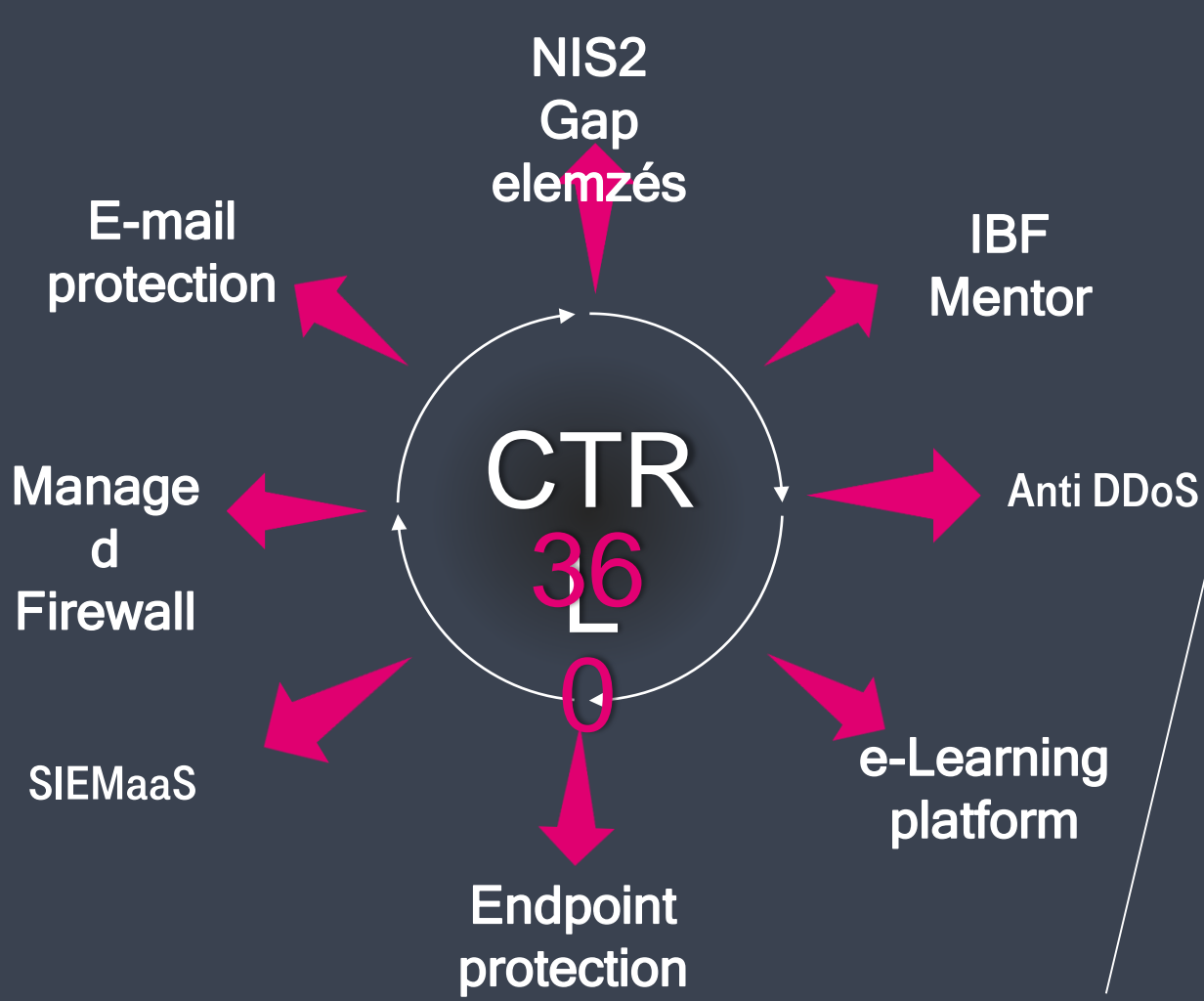
CTI használati esetek a
SOC és SWAT
szolgáltatásainkban



Hlavaty Győző

Magyar Telekom
SOC központ vezető

Telekom Managed Cybersecurity Services



CTI – Gyártók, partnerek



MSSP partnerség



Sodan, HackerTarget, Virustotal, HavelbeenPwned ...

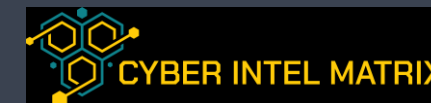
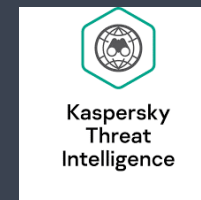


Belső IOC-k és Brand monitoring



Fortinet FortiGuard, Trellix GTI
Trend Micro Threat Intelligence

...



CYBER THREAT RESILIENCE TEAM BY 

SOC használati esete

- Threat landscape
- Malware outbreak információk
- Brand monitoring riasztások
- CTI alertek
- Beszállítói lánc figyelése
- Honeypot adatok
- Sérülékenységi információk
- TTP-k és IOC-k

CTRL

CYBER THREAT RESILIENCE T



SWAT használati esetek

- Leaked credentials
- Malware logs
- IP és Domain információk
- APT csoportok és jellemzőik
- Malware leírások
- TTP-k és IOC-k
- Sérülékenységi információk
- Hasznos hivatkozások
- ...bárhon, bármikor

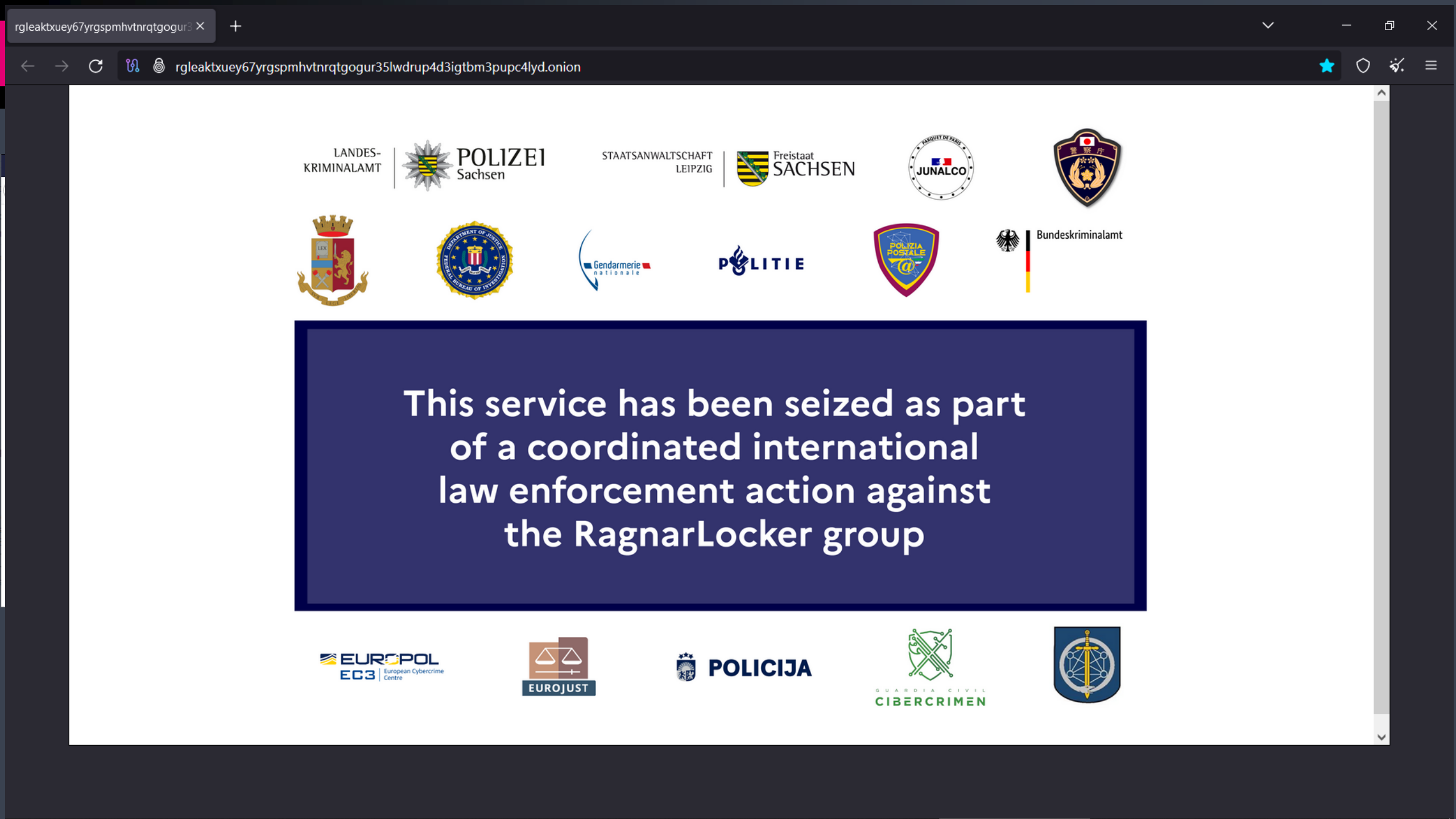
CTRL

CYBER THREAT RESILIENCE TEAM B

The screenshot displays the Recorded Future mobile application interface. At the top, the status bar shows the time 19:31 and battery level at 100%. The app header includes the Recorded Future logo and a search icon. The main content area features a risk score of 29 out of 100, labeled as 'Suspicious', with 5 of 77 risk rules triggered. Below this, a table provides key details:

Total References	1 000+	Insikt Group Research	0
First Reference	Dec 14, 2023, 00:51	Latest Reference	Apr 30, 2024, 05:06
ASN	AS396982	GEO	Kansas City
ORG	GOOGLE-CLOUD-PLATFORM		

Below the table, an AI Insights section states: "The IP address 34.117.186.192 has been identified by the Proofpoint Reputation Feed as being associated with adware and spyware activities, specifically used to report user activity on April 22, 2024. This indicates that the IP address is linked to malicious behavior aimed at monitoring and potentially compromising us... See More". At the bottom, a section titled "Triggered Risk Rules" is visible, along with a navigation bar containing icons for News, Research, Alerts, AI, Search, and Settings.



LANDES-KRIMINALAMT



POLIZEI Sachsen

STAATSANWALTSCHAFT LEIPZIG



This service has been seized as part of a coordinated international law enforcement action against the RagnarLocker group





Hlavaty Győző
SOC központ vezető
hlavaty.gyozo@telekom.h
u



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