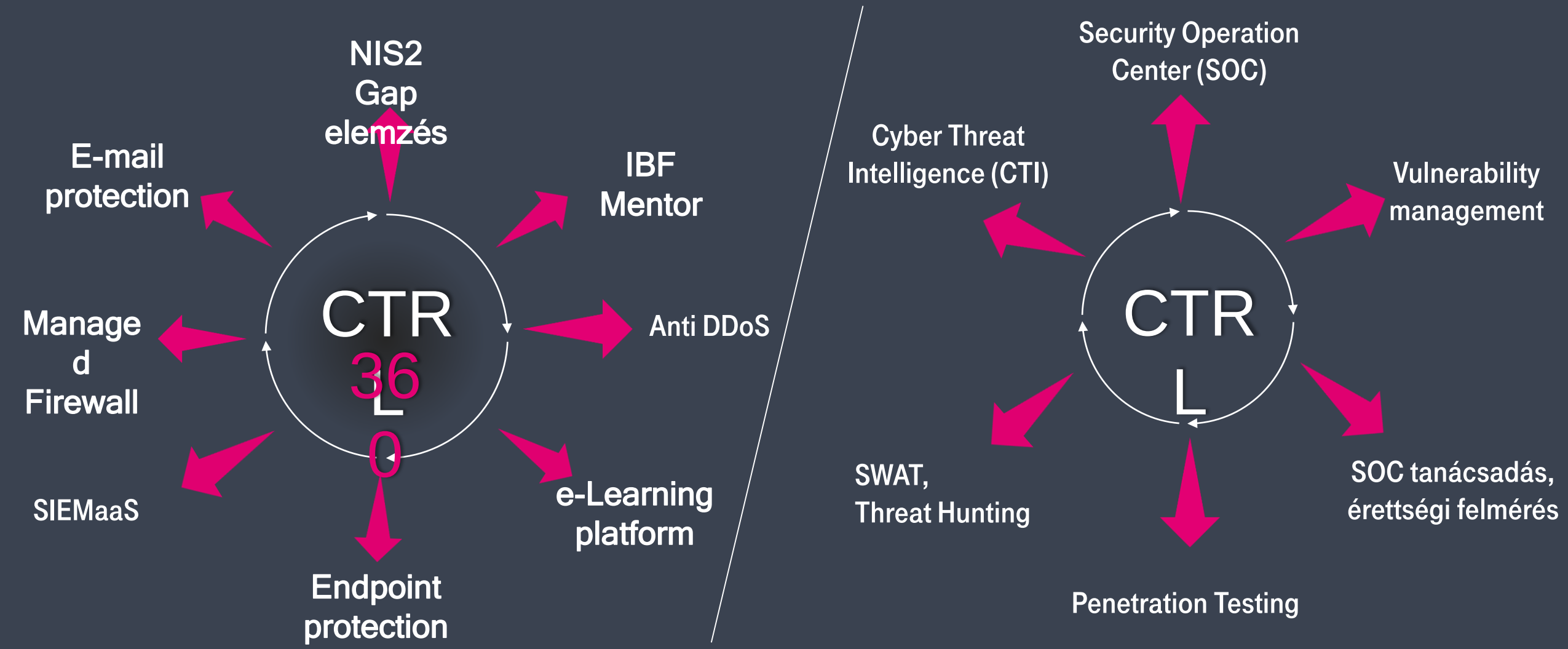
CTI használati esetek a SOC és SWAT szolgáltatásainkban

Hlavaty Győző
Magyar Telekom
SOC központ vezető

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

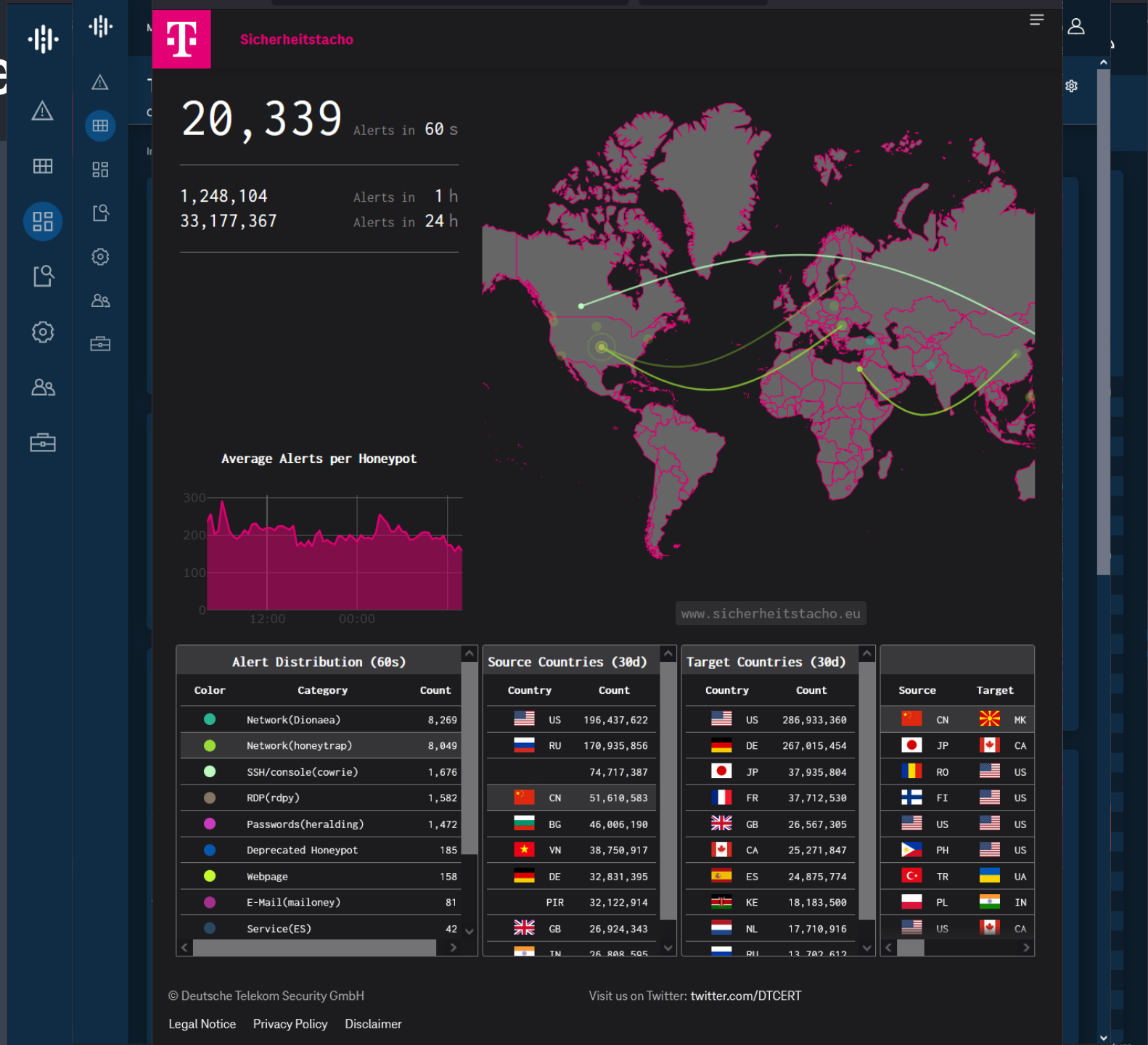
CYBER INTEL MATRIX

MANDIANT

SOC használati 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

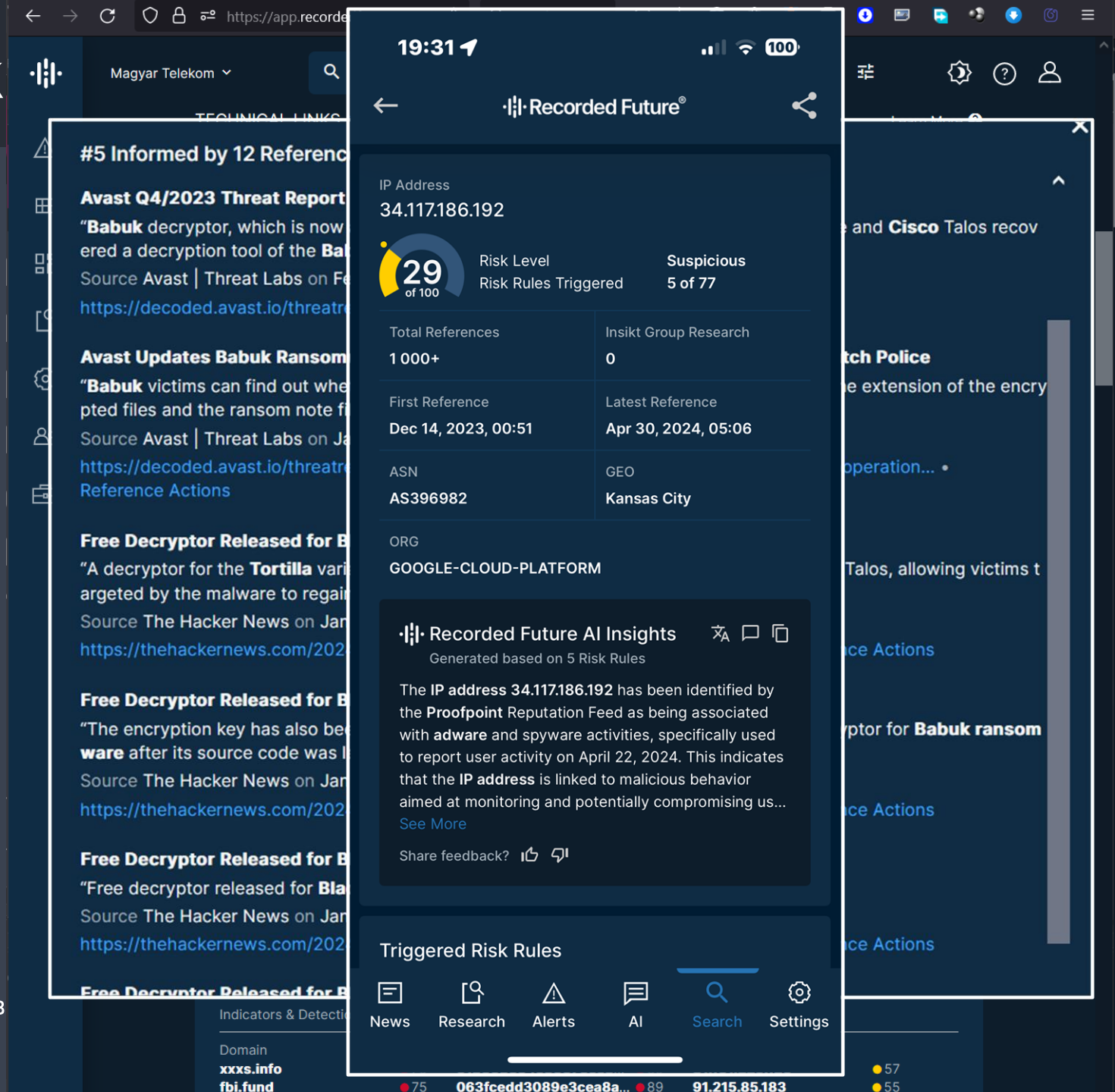


SWAT használati esetek

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

- ...bárhol, bármikor

CTRL CYBER THREAT RESILIENCE TEAM B



T Business

Hlavaty Győző
SOC központ vezető
hlavaty.gyozo@telekom.hu

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