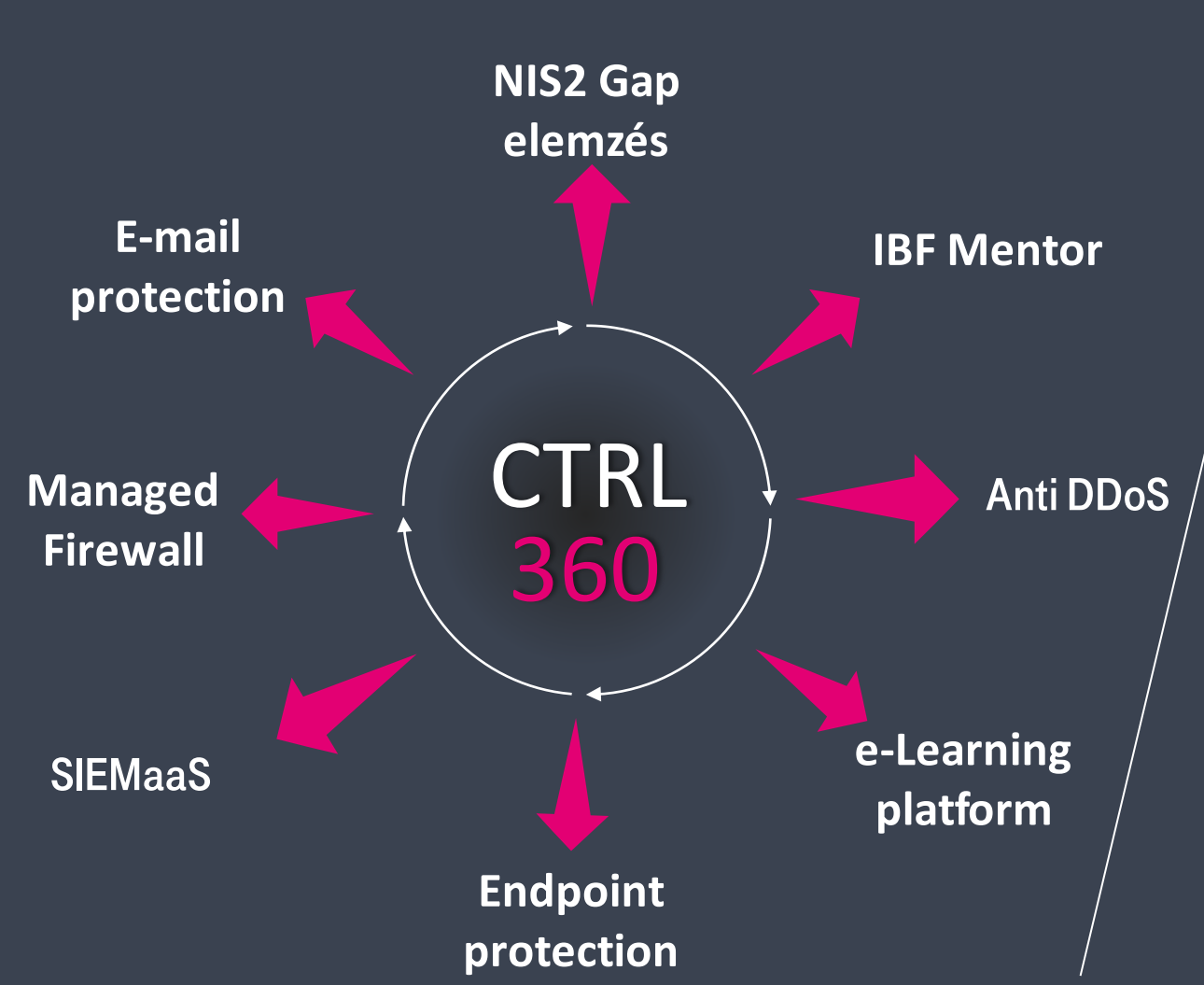
CTI használati esetek a SOC és SWAT szolgáltatásainkban

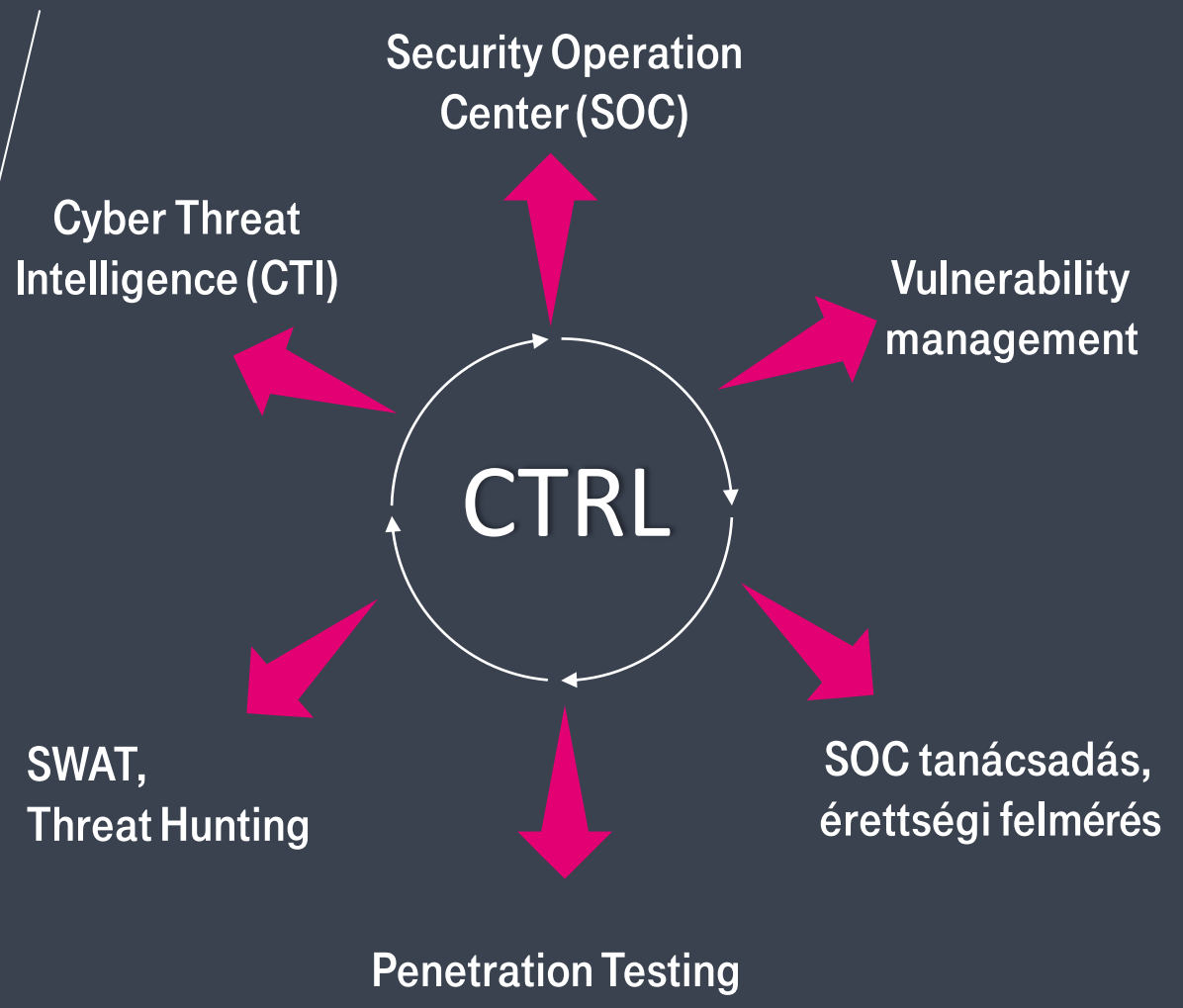
Hlavaty Győző

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 esetek

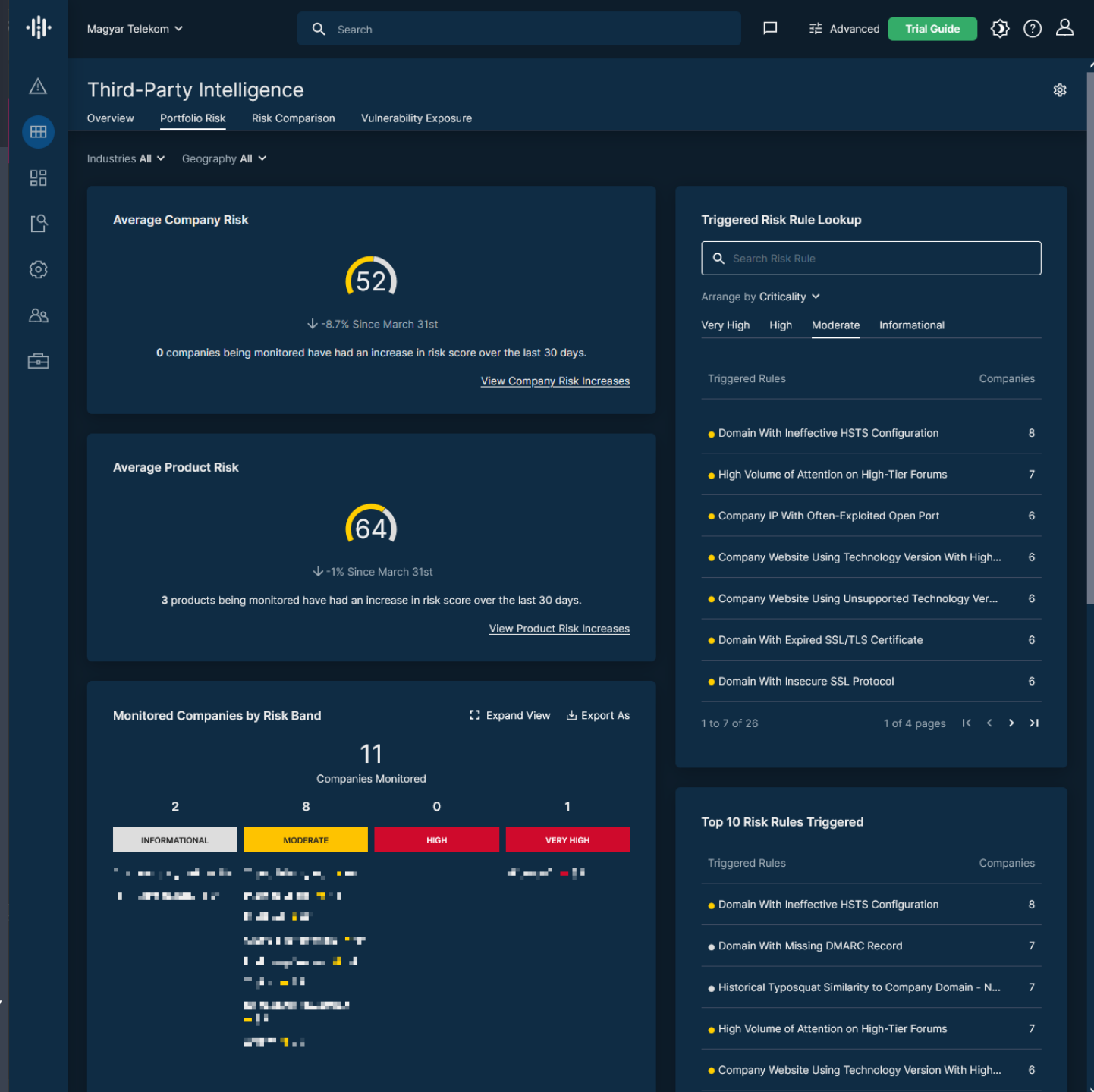
- Threat landscape

CTRL CYBER THREAT RESILIENCE TEAM

SOC használati esetek

- Threat landscape
- Malware outbreak információk
- Brand monitoring riasztások
- CTI alertek
- Beszállítói lánc figyelése

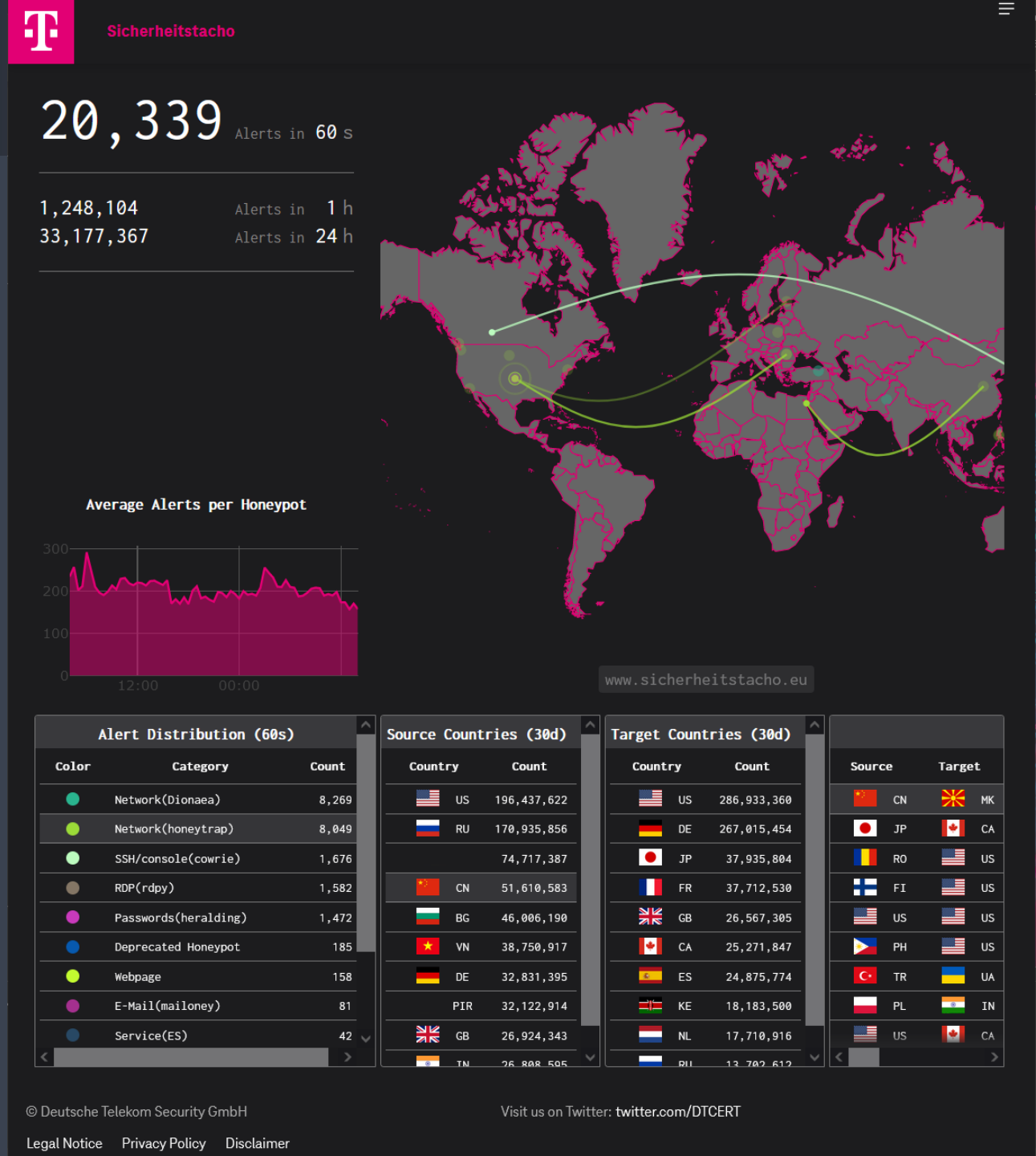
CTRL CYBER THREAT RESILIENCE TEAM BY



SOC használati esetek

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

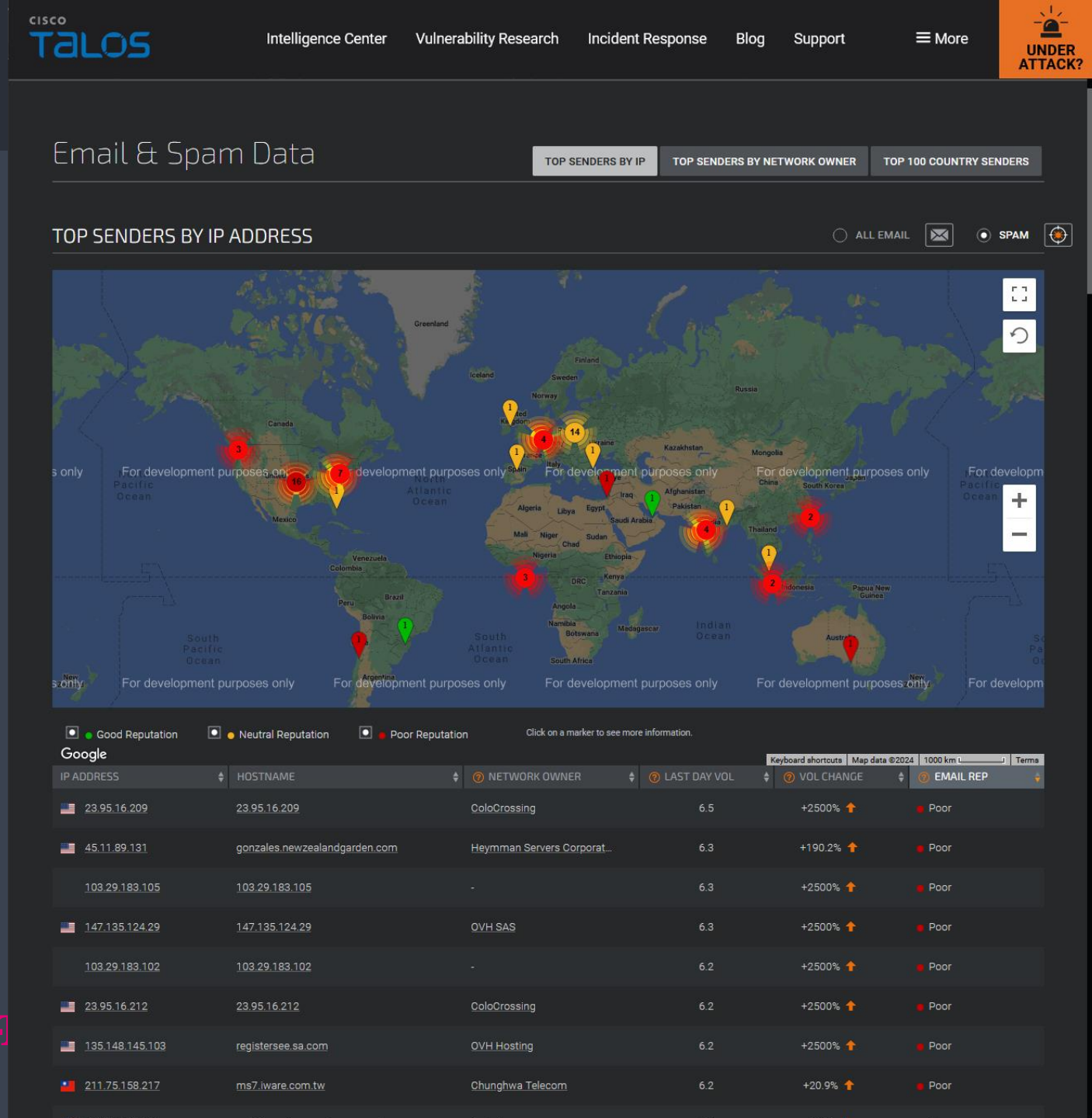
CTRL CYBER THREAT RESILIENCE TEAM BY T



SWAT használati esetek

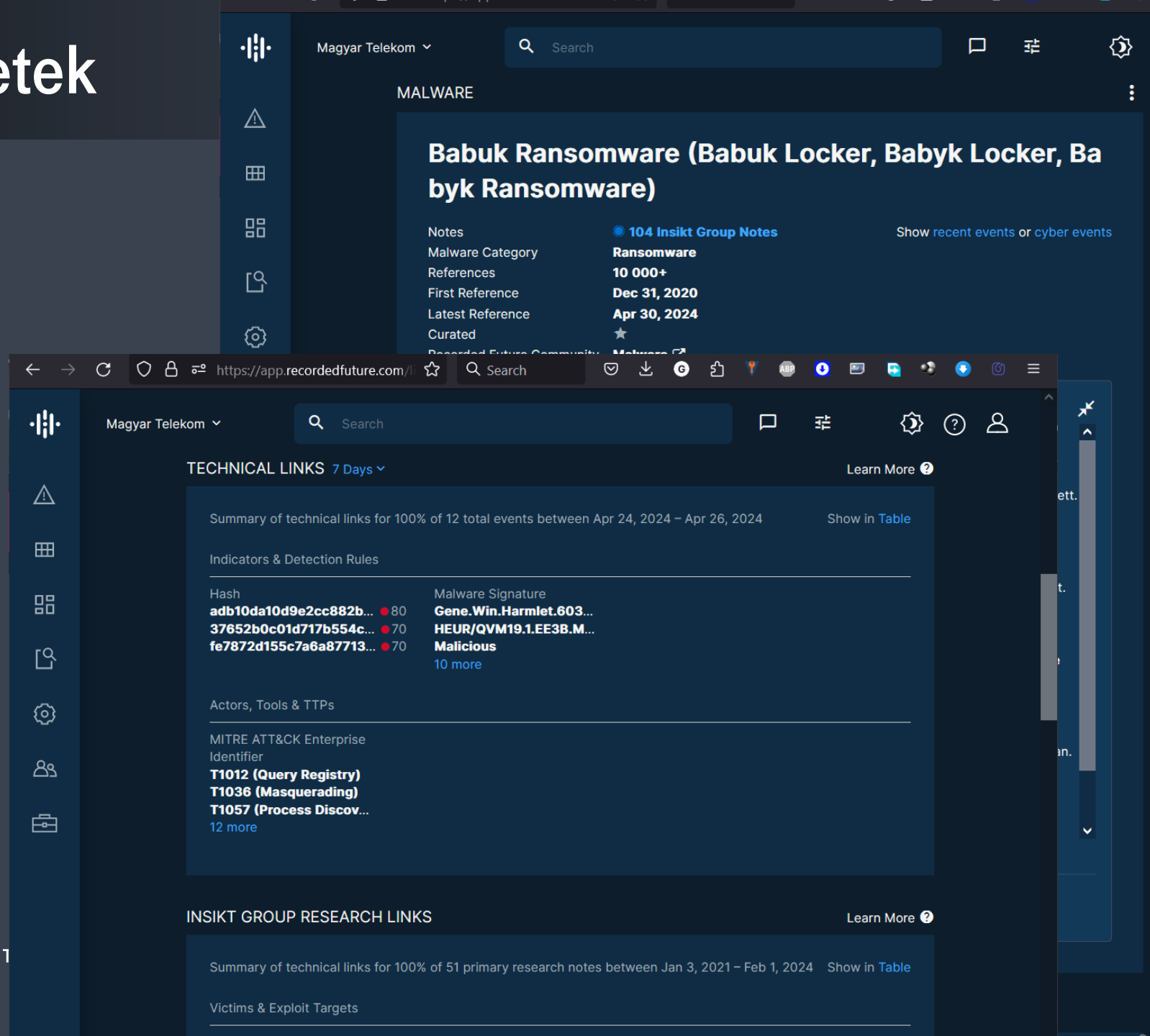
- Leaked credentials
- Malware logs
- IP és Domain információk

CTRL CYBER THREAT RESILIENCE TEAM BY



SWAT használati esetek

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



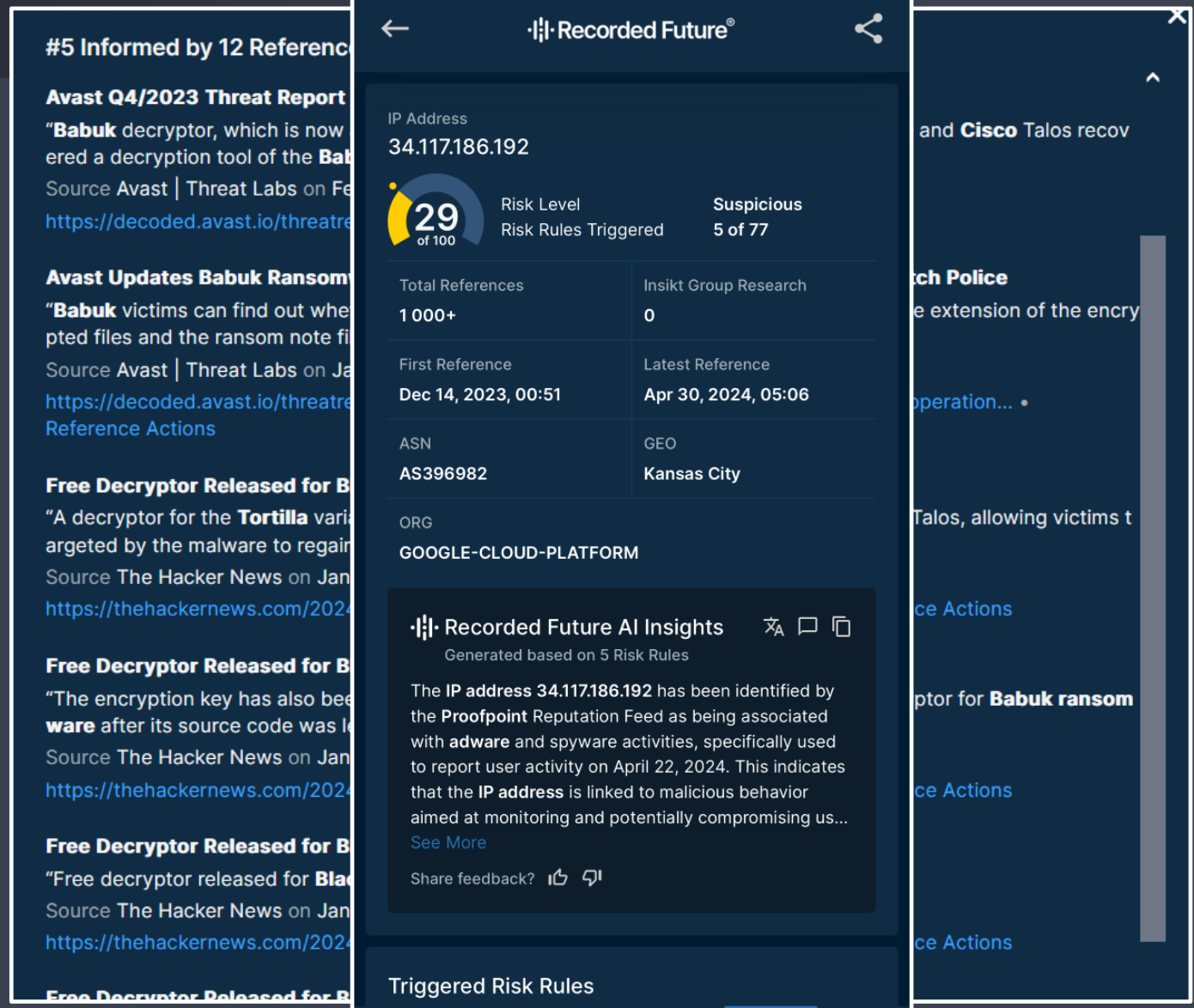
CTRL CYBER THREAT RESILIENCE T

SWAT használati esetek

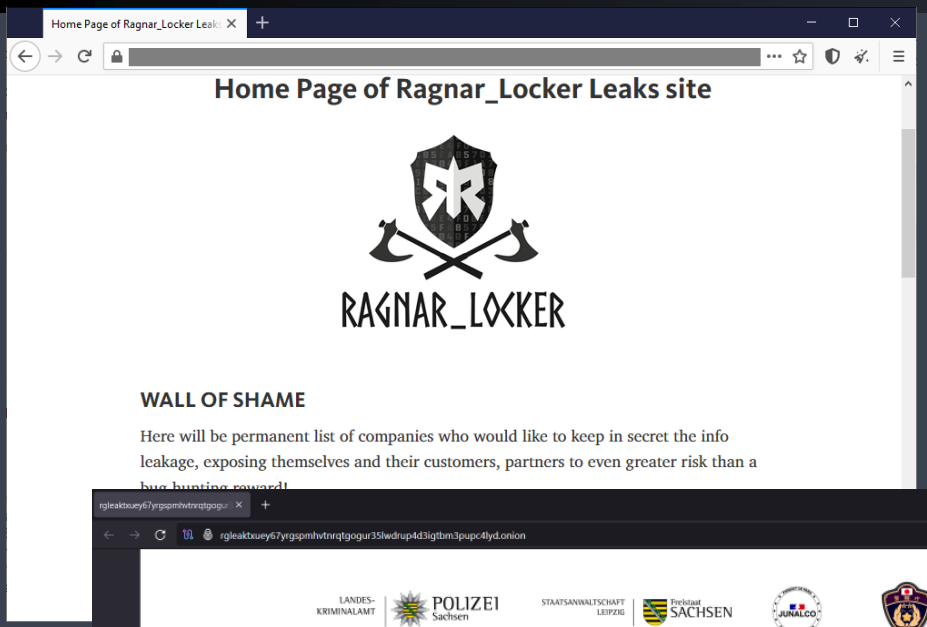
- Leaked credentials
- Malware logs
- IP és Domain információk
- APT csoportok és jellemzőik
- Malware leírások
- TTP-k és IOC-k
- Sérülékenységi információk
- Hasznos hivatkozások

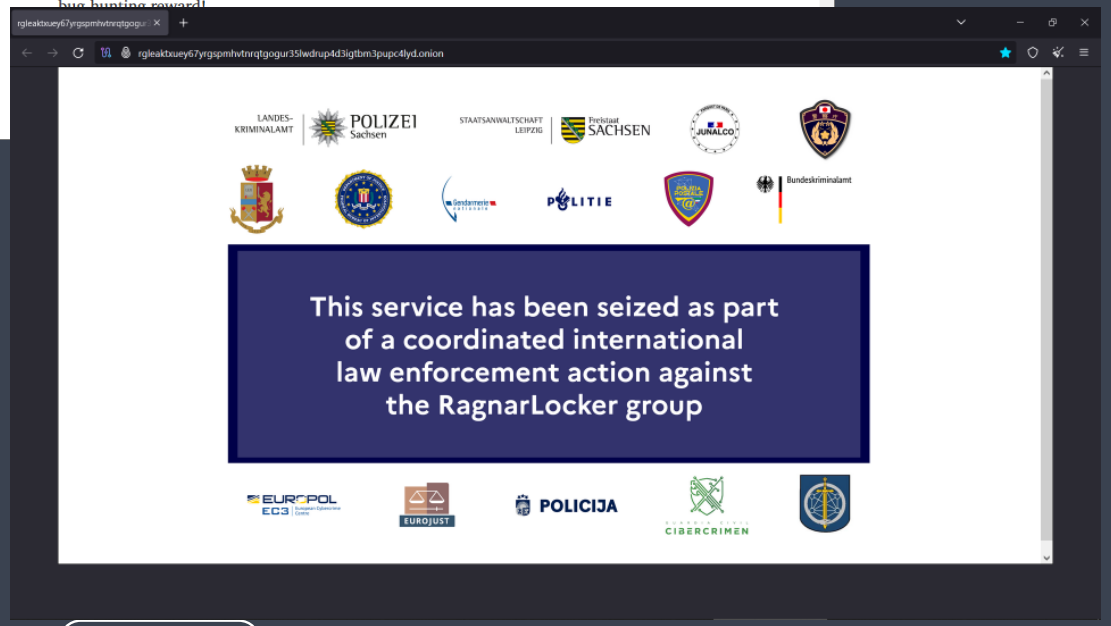
- ...bárhol, bármikor

CTRL CYBER THREAT RESILIENCE TEAM BY T



Tapasztalatok





- Napról napra változó adatok és szolgáltatások
- Drága szolgáltatás

- Nagyon sok adat elérhető a CTI forrásokban
- Sok a kiszivárgott felhasználói adat
- Sikeres támadásról néhány nap alatt értesülünk
- Hasznos, hogy tudjuk, mi lehet a támadók kezében

- OSINT elmozdult fizetős irányba
- A gyártói feedek csak az adott technológiákra használhatóak

- Kicsi az ország, kicsik a cégek – kevés az információ
- A scoreing nagyon más mindenhol

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

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