

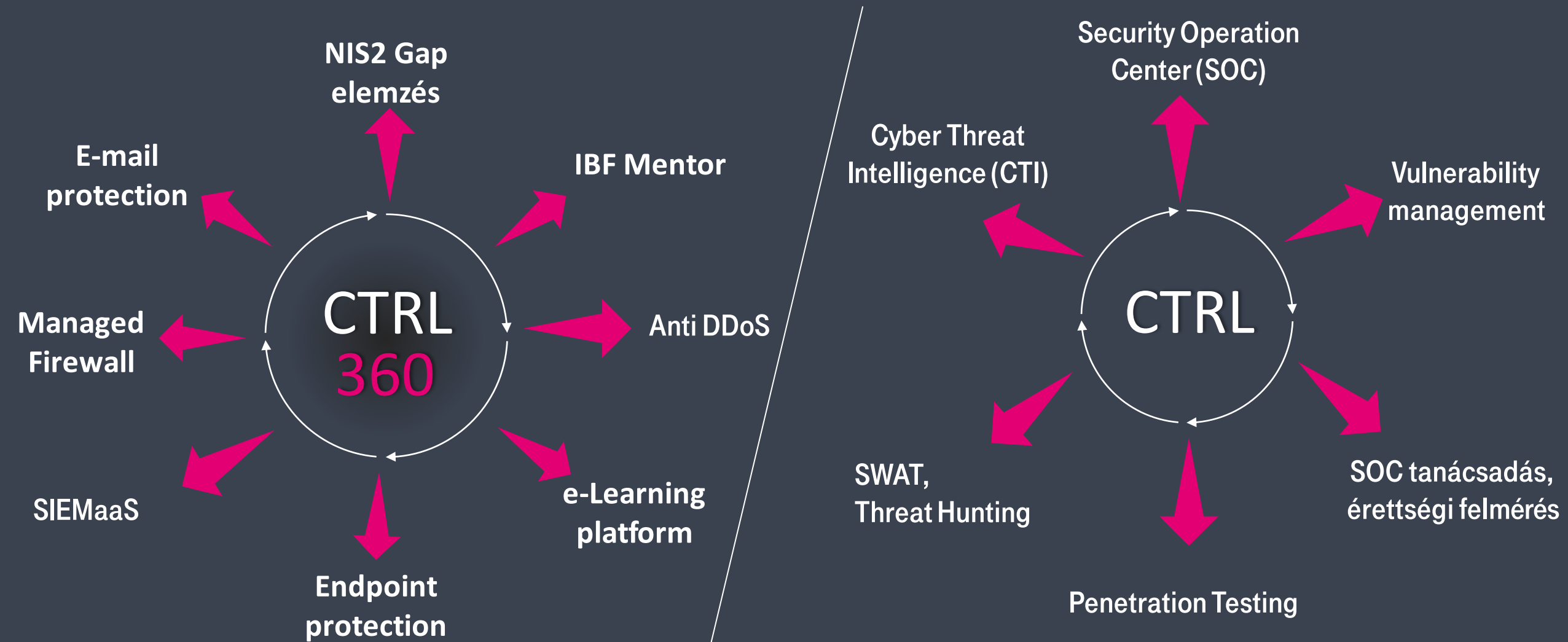
CTI használati esetek a SOC és SWAT szolgáltatásainkban



Hlavaty Győző

Magyar Telekom
SOC központ vezető

Telekom Managed Cybersecurity Services



CYBER THREAT RESILIENCE TEAM BY 

CTI – Gyártók, partnerek



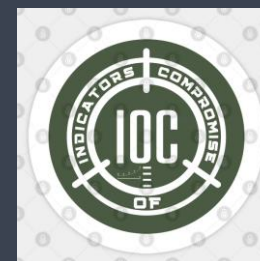
MSSP partnerség



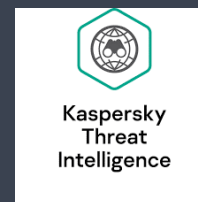
Sodan, HackerTarget,
VirusTotal, HavelbeenPwned ...



Belső IOC-k és Brand monitoring



Fortinet FortiGuard, Trellix GTI
Trend Micro Threat Intelligence
...



CYBER THREAT RESILIENCE TEAM BY 

SOC használati esetek

Threat landscape



CYBER THREAT RESILIENCE TEAM

SOC használati esetek

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



CYBER THREAT RESILIENCE TEAM BY

The screenshot displays a security dashboard with the following sections:

- Third-Party Intelligence**: Overview, Portfolio Risk, Risk Comparison, Vulnerability Exposure. Filters: Industries All, Geography All.
- Average Company Risk**: Score 52, -8.7% Since March 31st. 0 companies being monitored have had an increase in risk score over the last 30 days. [View Company Risk Increases](#)
- Average Product Risk**: Score 64, -1% Since March 31st. 3 products being monitored have had an increase in risk score over the last 30 days. [View Product Risk Increases](#)
- Monitored Companies by Risk Band**: 11 Companies Monitored. Legend: INFORMATIONAL (2), MODERATE (8), HIGH (0), VERY HIGH (1).
- Triggered Risk Rule Lookup**: Search Risk Rule. Arrange by Criticality: Very High, High, Moderate, Informational. Table:

Triggered Rules	Companies
Domain With Ineffective HSTS Configuration	8
High Volume of Attention on High-Tier Forums	7
Company IP With Often-Exploited Open Port	6
Company Website Using Technology Version With High...	6
Company Website Using Unsupported Technology Ver...	6
Domain With Expired SSL/TLS Certificate	6
Domain With Insecure SSL Protocol	6
- Top 10 Risk Rules Triggered**: Table:

Triggered Rules	Companies
Domain With Ineffective HSTS Configuration	8
Domain With Missing DMARC Record	7
Historical Typosquat Similarity to Company Domain - N...	7
High Volume of Attention on High-Tier Forums	7
Company Website Using Technology Version With High...	6

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

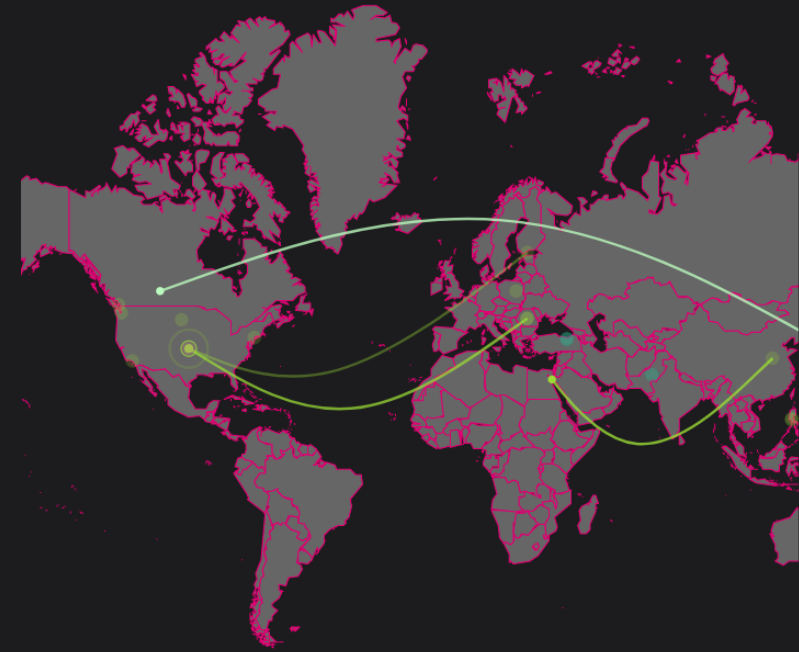


Sicherheitstacho

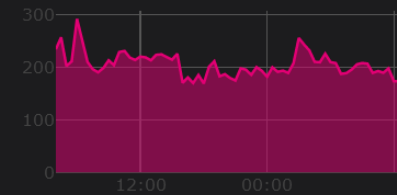
20,339 Alerts in 60 s

1,248,104 Alerts in 1 h

33,177,367 Alerts in 24 h



Average Alerts per Honeypot



www.sicherheitstacho.eu

Alert Distribution (60s)		
Color	Category	Count
●	Network(Dionaea)	8,269
●	Network(honeytrap)	8,049
●	SSH/console(cowrie)	1,676
●	RDP(rdp)	1,582
●	Passwords(heralding)	1,472
●	Deprecated Honeypot	185
●	Webpage	158
●	E-Mail(mailoney)	81
●	Service(ES)	42

Source Countries (30d)		
Country	Count	
US	196,437,622	
RU	170,935,856	
	74,717,387	
CN	51,610,583	
BG	46,006,190	
VN	38,750,917	
DE	32,831,395	
PIR	32,122,914	
GB	26,924,343	
TN	26,888,595	

Target Countries (30d)		
Country	Count	
US	286,933,360	
DE	267,015,454	
JP	37,935,804	
FR	37,712,530	
GB	26,567,305	
CA	25,271,847	
ES	24,875,774	
KE	18,183,500	
NL	17,710,916	
RU	13,702,612	

Source	Target
CN	MK
JP	CA
RO	US
FI	US
US	US
PH	US
TR	UA
PL	IN
US	CA



SWAT használati esetek

- Leaked credentials
- Malware logs
- IP és Domain információk



CYBER THREAT RESILIENCE TEAM BY

Email & Spam Data

TOP SENDERS BY IP TOP SENDERS BY NETWORK OWNER TOP 100 COUNTRY SENDERS

TOP SENDERS BY IP ADDRESS

ALL EMAIL SPAM



Good Reputation Neutral Reputation Poor Reputation

Click on a marker to see more information.

Google

IP ADDRESS	HOSTNAME	NETWORK OWNER	LAST DAY VOL	VOL CHANGE	EMAIL REP
23.95.16.209	23.95.16.209	ColoCrossing	6.5	+2500%	Poor
45.11.89.131	gonzales.newzealandgarden.com	Heymman Servers Corporat..	6.3	+190.2%	Poor
103.29.183.105	103.29.183.105	-	6.3	+2500%	Poor
147.135.124.29	147.135.124.29	OVH SAS	6.3	+2500%	Poor
103.29.183.102	103.29.183.102	-	6.2	+2500%	Poor
23.95.16.212	23.95.16.212	ColoCrossing	6.2	+2500%	Poor
135.148.145.103	registersee.sa.com	OVH Hosting	6.2	+2500%	Poor
211.75.158.217	ms7.iware.com.tw	Chunghwa Telecom	6.2	+20.9%	Poor

SWAT használati esetek

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

The screenshot shows the Recorded Future interface for a Malware entry. The entry is titled "Babuk Ransomware (Babuk Locker, Babyk Locker, Babyk Ransomware)". It includes a "Notes" section with "104 Insikt Group Notes", a "Malware Category" of "Ransomware", and "References" of "10 000+". The "First Reference" is dated "Dec 31, 2020" and the "Latest Reference" is "Apr 30, 2024". The interface also shows a search bar, a navigation menu, and a "Show recent events or cyber events" link.

The screenshot shows the Recorded Future interface for "TECHNICAL LINKS" and "INSIKT GROUP RESEARCH LINKS". The "TECHNICAL LINKS" section is for "7 Days" and shows a summary of technical links for 100% of 12 total events between Apr 24, 2024 – Apr 26, 2024. It includes a table of Indicators & Detection Rules with columns for Hash, Malware Signature, and Malicious. The "Actors, Tools & TTPs" section lists MITRE ATT&CK Enterprise Identifier: T1012 (Query Registry), T1036 (Masquerading), and T1057 (Process Discov...). The "INSIKT GROUP RESEARCH LINKS" section shows a summary of technical links for 100% of 51 primary research notes between Jan 3, 2021 – Feb 1, 2024. It includes a table of Victims & Exploit Targets.

Hash	Malware Signature	Malicious
adb10da10d9e2cc882b...	Gene.Win.Harmlet.603...	10 more
37852b0c01d717b554c...	HEUR/QVM19.1.EE3B.M...	
fe7872d155c7a6a87713...	Malicious	

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

#5 Informed by 12 Reference

Avast Q4/2023 Threat Report
"Babuk decryptor, which is now...
ered a decryption tool of the Babuk...
Source Avast | Threat Labs on Fe...
<https://decoded.avast.io/threatre...>

Avast Updates Babuk Ransom
"Babuk victims can find out whe...
pted files and the ransom note fil...
Source Avast | Threat Labs on Ja...
<https://decoded.avast.io/threatre...>
Reference Actions

Free Decryptor Released for B
"A decryptor for the **Tortilla** varia...
argeted by the malware to regain...
Source The Hacker News on Jan...
<https://thehackernews.com/2024...>

Free Decryptor Released for B
"The encryption key has also bee...
ware after its source code was le...
Source The Hacker News on Jan...
<https://thehackernews.com/2024...>

Free Decryptor Released for B
"Free decryptor released for **Blac**...
Source The Hacker News on Jan...
<https://thehackernews.com/2024...>

Free Decryptor Released for B

19:31

Recorded Future®

IP Address
34.117.186.192

Risk Level
29 of 100
Risk Rules Triggered
Suspicious
5 of 77

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

Recorded Future AI Insights
Generated based on 5 Risk Rules

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](#)

Share feedback?

Triggered Risk Rules

News Research Alerts AI Search Settings

and **Cisco** Talos recov

ch Police
e extension of the encry

operation...

Talos, allowing victims t

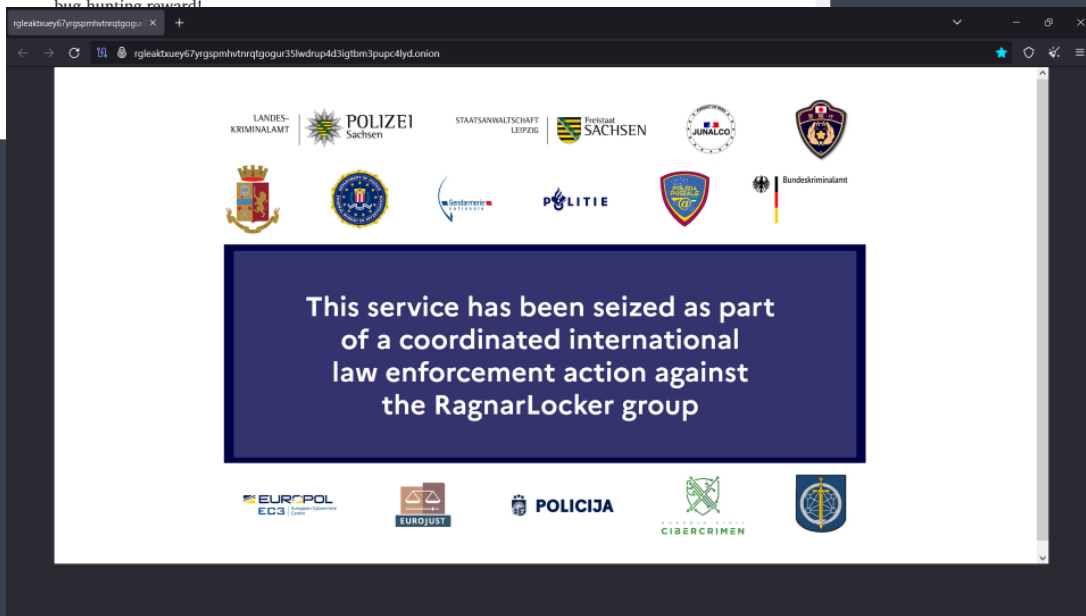
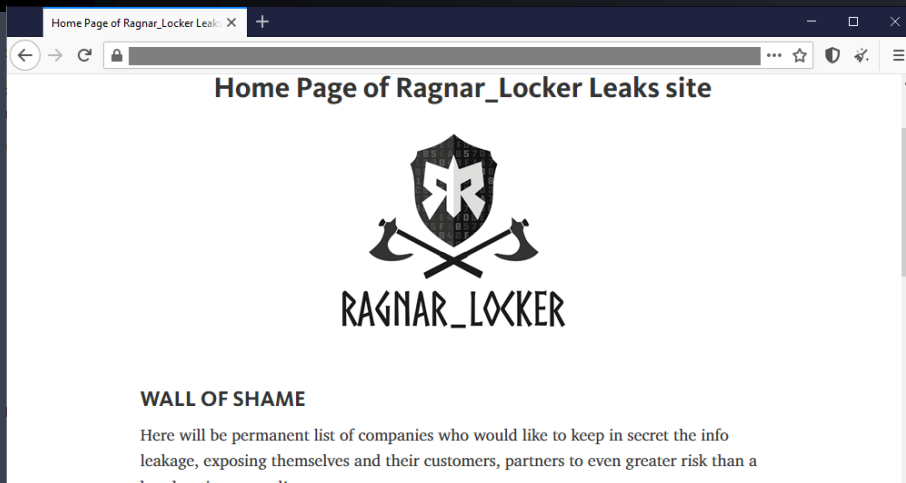
ce Actions

ptor for **Babuk** ransom

ce Actions

ce Actions

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