

CTRL

CYBER THREAT RESILIENCE TEAM

BY 

CTRL – A TELEKOM SIEM ÉS SOC SZOLGÁLTATÁSA

- 2000 SIEM implementációk
- 2010 MIBS
- 2014 SIEM as a Service
- 2017 7x24 SOC
- Dedikált fizikai helyszín
- Speciális informatikai környezet
- Dedikált kollégák
- 7x24-es műszakos munkarend



CTRL

CYBER THREAT RESILIENCE TEAM

BY T

MEGELŐZÉS

DETEKTÁLÁS

INCIDENSKEZELÉS

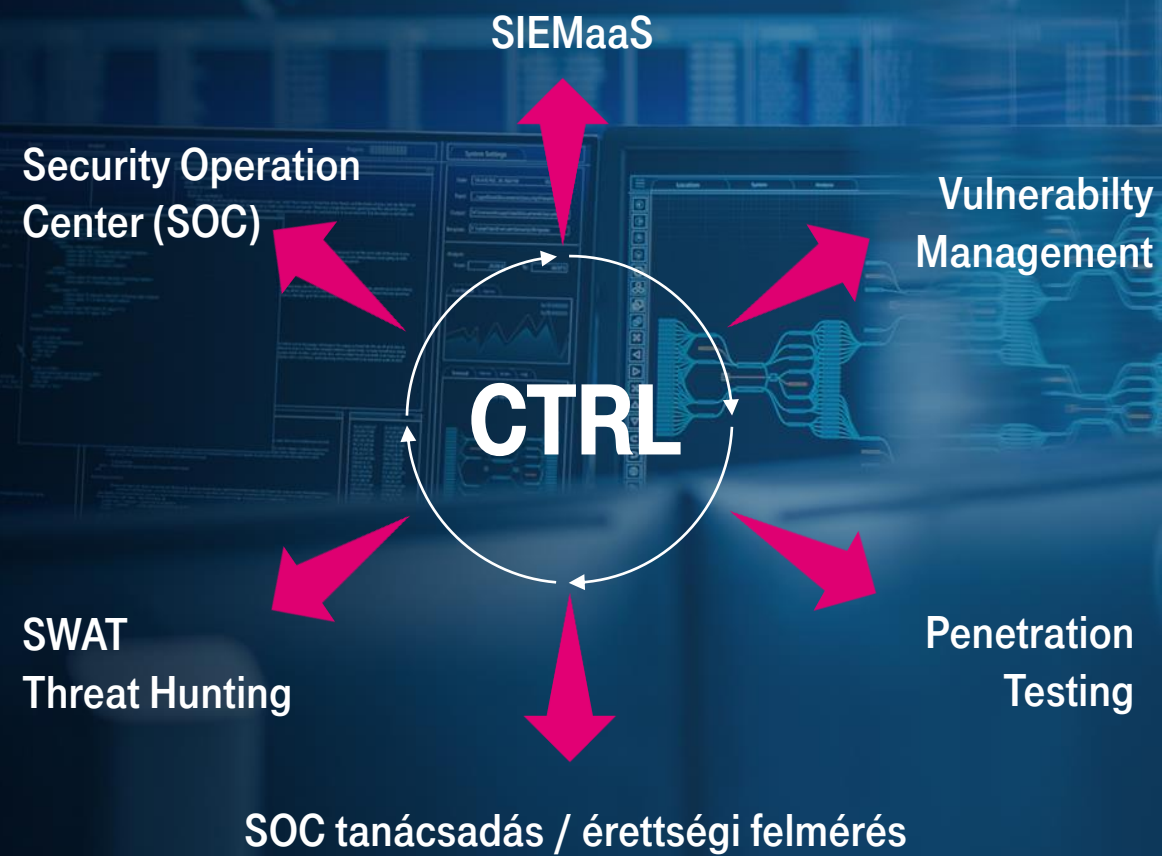
KRÍZISKEZELÉS

POSZT-INCIDENS
ANALÍZIS





Telekom CTRL



Előnyök

- Minden adat helyben marad
- Belső rendszerek mély ismerete
- Gördülékenyebb együttműködés
- Mélyebb szintű testreszabás
- Dedikált személyzet

Hátrányok

- Magas indulási és bővítési CAPEX
- Eredményeket kell hozni azonnal
- Elfogult
- Nagyobb az esély együttműködésre az támadó és az elemző között
- Kevés tapasztalat
- Emberhiány

Előnyök

- Minimális CAPEX igény
- Komoly szakértelem
- Sok tapasztalat
- Elfogulatlan
- Nem kell plusz szakember
- Jól skálázható és rugalmas
- SLA

Hátrányok

- A szakértő „külsős”
- A kiszervezés csökkentheti a morált
- Hiányzik a belső szakértelem
- Az adatok külső cégnél tárolódhatnak
- A szolgáltatók standardizálnak



CTRL SOC

Dedikált helyszín

Specializálódott kollégák

Fizikai védelem

IT biztonság

Transzparencia, auditálhatóság

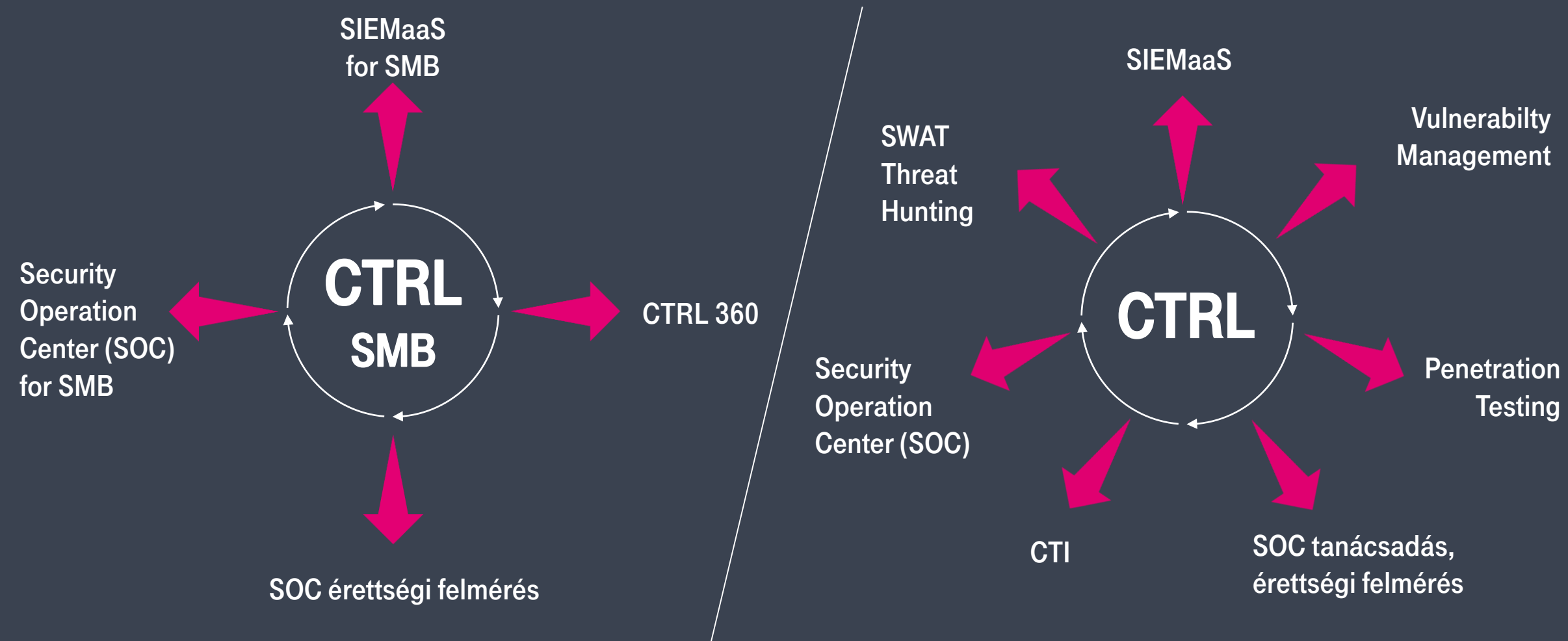
Folyamat alapú működés

Ügyfelekre szabott eljárásrendek és folyamatok

Rugalmasság

Szoros együttműködés az ügyfelekkel

Cybersecurity services



CTRL

CYBER THREAT RESILIENCE TEAM BY 

CTRL

CYBER THREAT RESILIENCE TEAM

BY 

HUMÁNFAKTOR ÉS TUDÁSBÁZIS

HR-szemponatok

- L1 – L2 – L3 rendszer
- Főállású SOC manager
- 7x24: műszakos munkarend
- Alapképzések, speciális képzések, folyamatos képzés
- Dinamikus emberallokáció lehetősége (C T R L – Telekom - DT)

Tudásbázis

- „Hozott” tudásra építhettünk
- Dedikált, a területre fókuszáló csapat
- Speciális, drága képzések
- TSM háttértámogatás
- Sok ügyfél – sok eset – sok tapasztalat
- Kiváló gyártói kapcsolatok – infók első kézből (pl. ransomware)



Security operation – Érettségi fok



1. Initial

- Log collecting
- Log monitoring,

2. Reactive

- SIEM
 - Baselines
 - Correlations
 - Historical analysis
- Dedicated group
- 7x24

3. Proactive

- SIEM integration
 - VS data
 - SD
 - ATD
 - Honeypot
- MITRE Framework

4. TI/Big data

- Threat Intelligence
- Big data analysis
- Anomaly detection
- UEBA

5. AI/SOAR

- Automated processes
- SOAR
- ML/AI

CTRL

CYBER THREAT RESILIENCE TEAM

BY T

SIEMaaS

Security Operation
Center (SOC)

Vulnerability
Management

CTRL

SWAT
Threat Hunting

Penetration
Testing

SOC tanácsadás / érettségi felmérés

