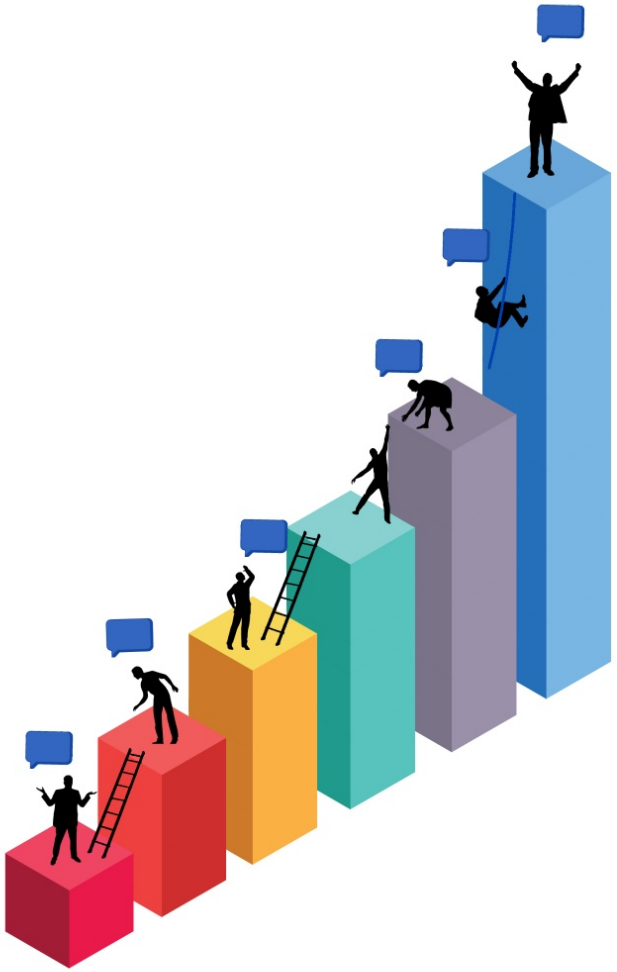
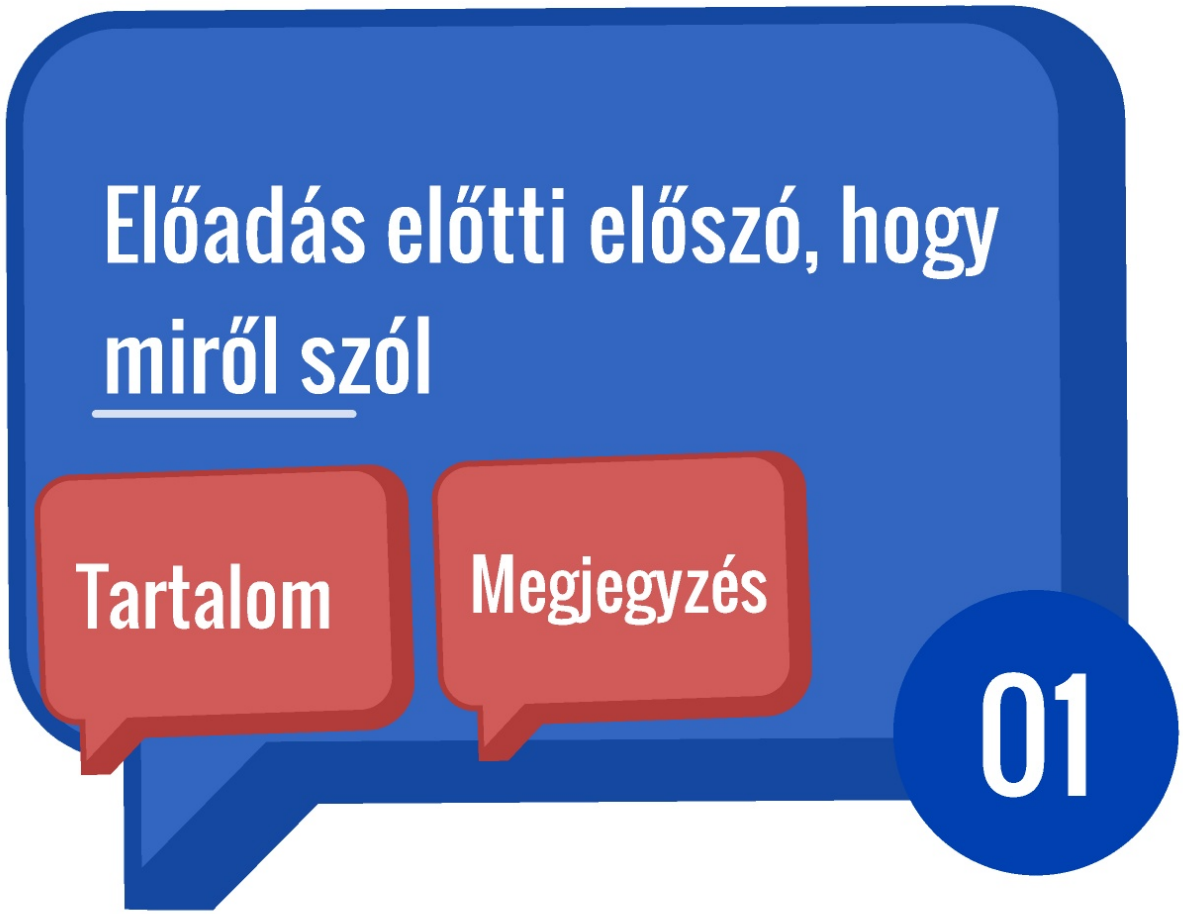
Rögzítendő jó

SOCaaS OK

avagy jó gyakorlatok kiberbiztonsági központokban

Ötvös Antal - CISSP, ISO 27001 CLA




Előadás előtti előszó, hogy miről szól
Tartalom
Megjegyzés
01

Az előadás tartalma

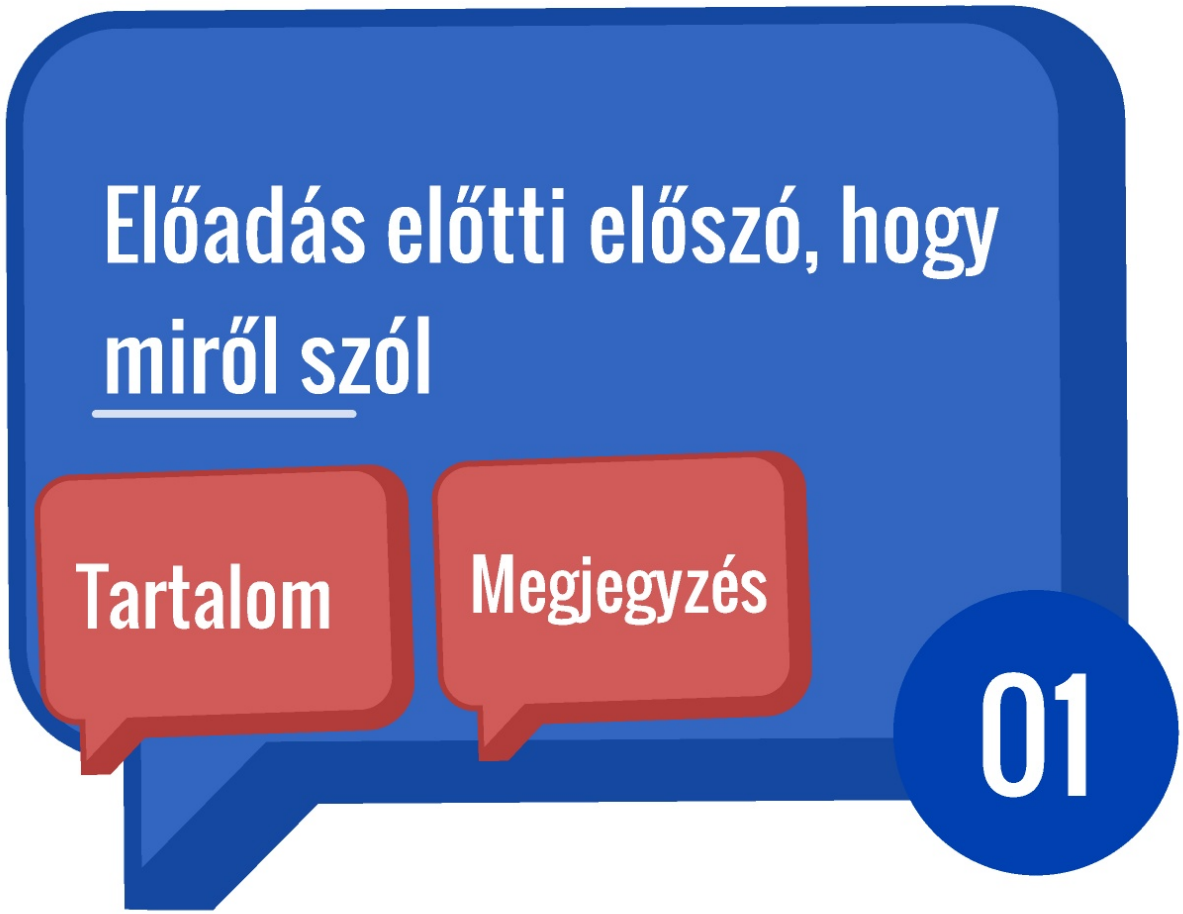
Alapfoglamak
- Kibertér, Kibervédelem

Kibervédelmi Központ - PPT modell alapján
- People, Process, Technology

Magyarországi Körkép - Versenyszféra

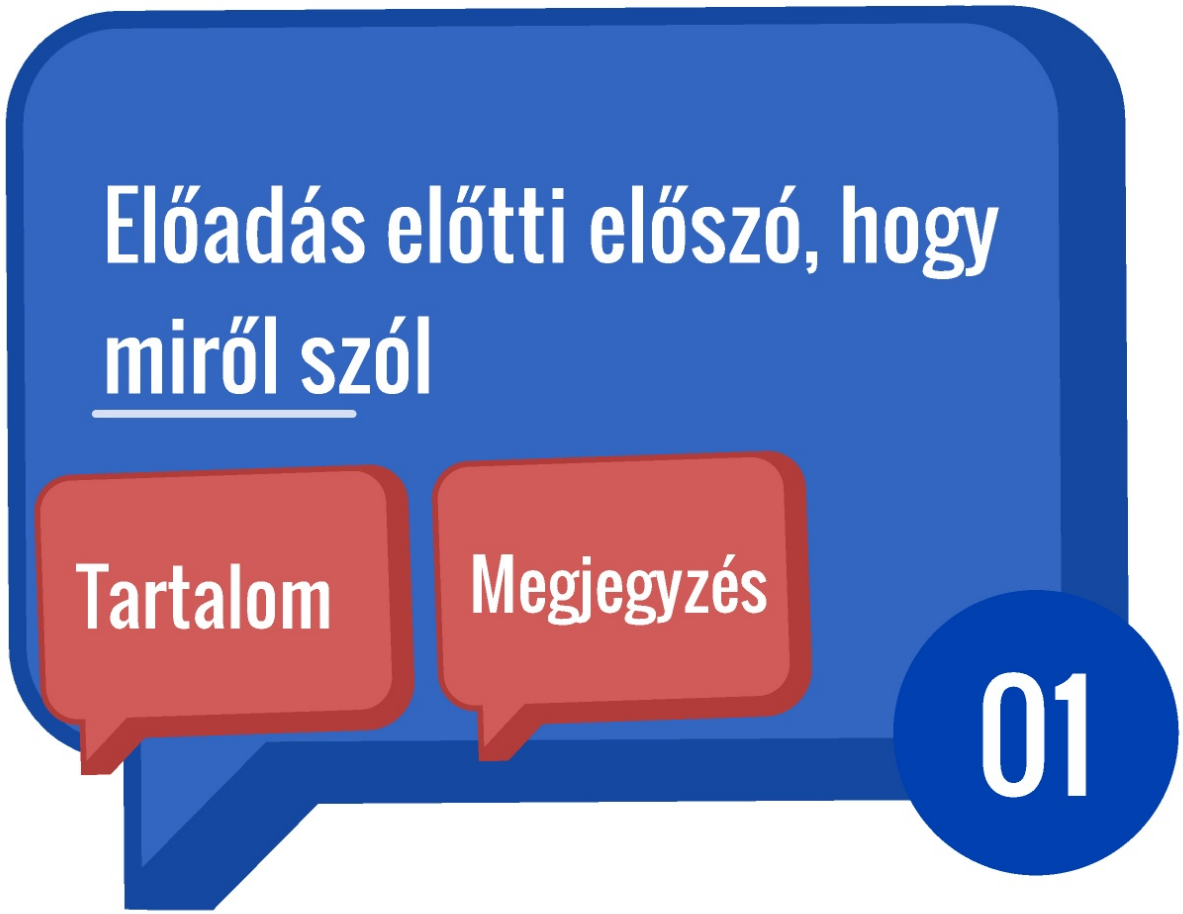
Kialakítandó jó SOCaaS-ok

Kérdések és Válaszok


Előadás előtti előszó, hogy miről szól
Tartalom
Megjegyzés
01

Megjegyzés az előadáshoz

Minden elhangzott információ, példa és minta a tankönyvekből, nyilvános forrásokból származó leírásokból, esetleg a képzeletem szüleményeiből származik, minden más a valósággal való bármilyen azonosság pusztán a véletlen műve.

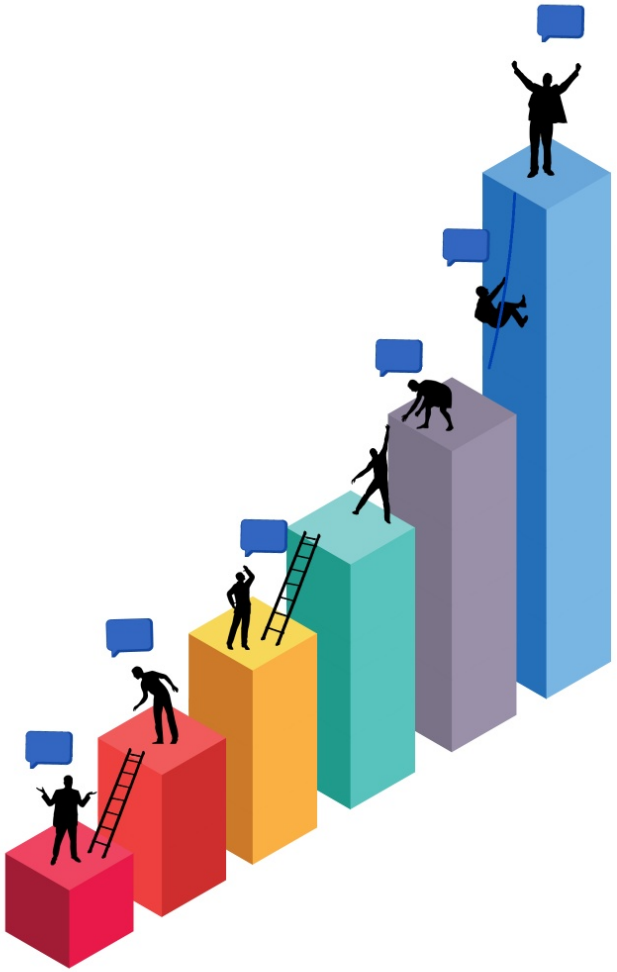

Előadás előtti előszó, hogy miről szól
Tartalom
Megjegyzés
01

Rögzítendő jó

SOCaaS OK

avagy jó gyakorlatok
kiberbiztonsági központokban

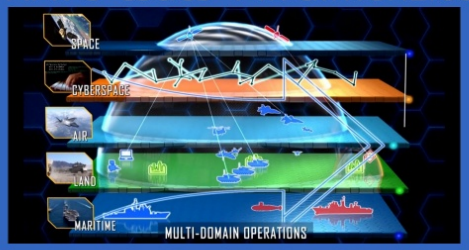
Ötvös Antal - CISSP, ISO 27001 CLA



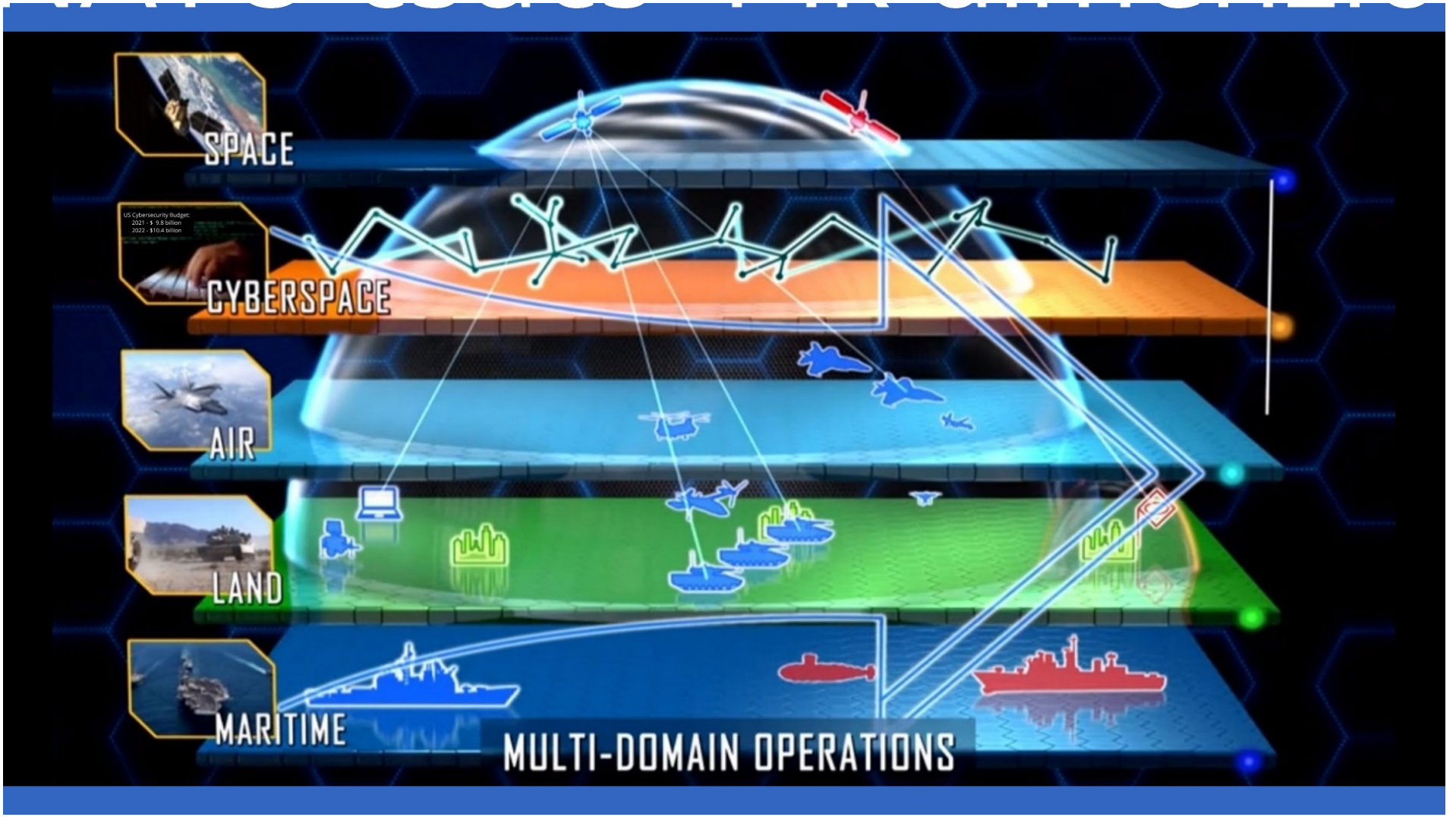
Alapfogalmak

Kibertér, Kiberbiztonság (Ibtv.)

2016 varsói NATO csúcs 4-ik dimenziós műveleti tér



02


SPACE
US Cybersecurity Budget:
2021 - $ 8.8 billion
2022 - $10.4 billion
CYBERSPACE
AIR
LAND
MARITIME
MULTI-DOMAIN OPERATIONS

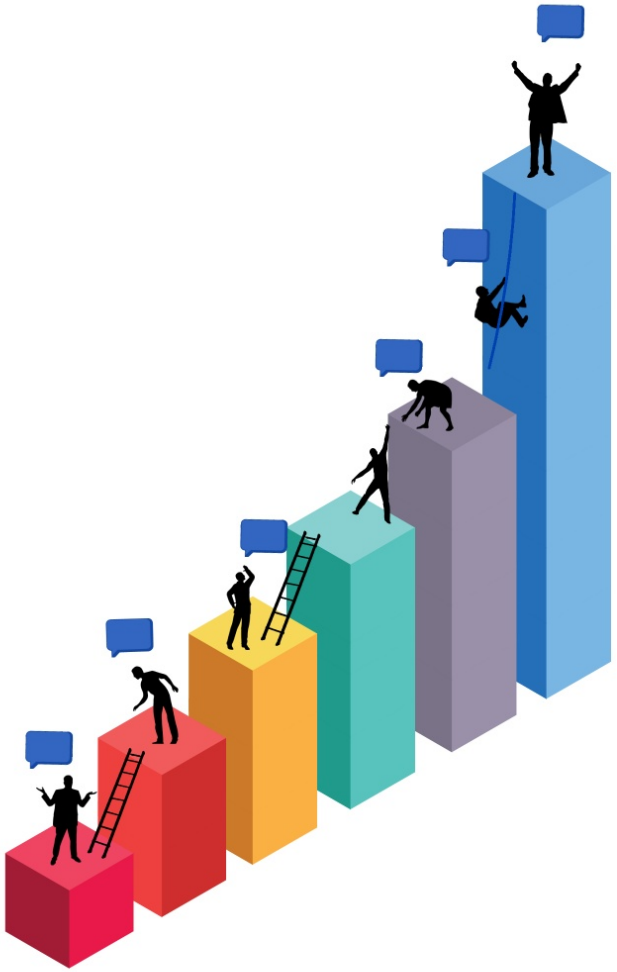

US Cybersecurity Budget:
2021 - $ 9.8 billion
2022 - $10.4 billion
CYBER

Rögzítendő jó

SOCaaS OK

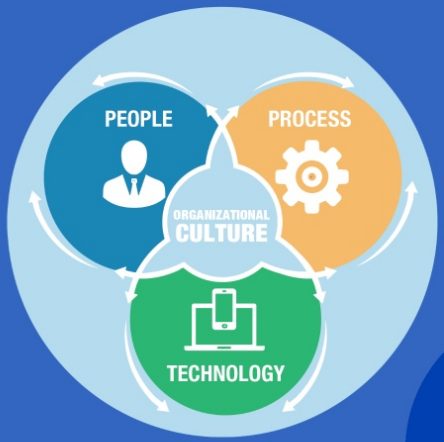
avagy jó gyakorlatok
kiberbiztonsági központokban

Ötvös Antal - CISSP, ISO 27001 CLA



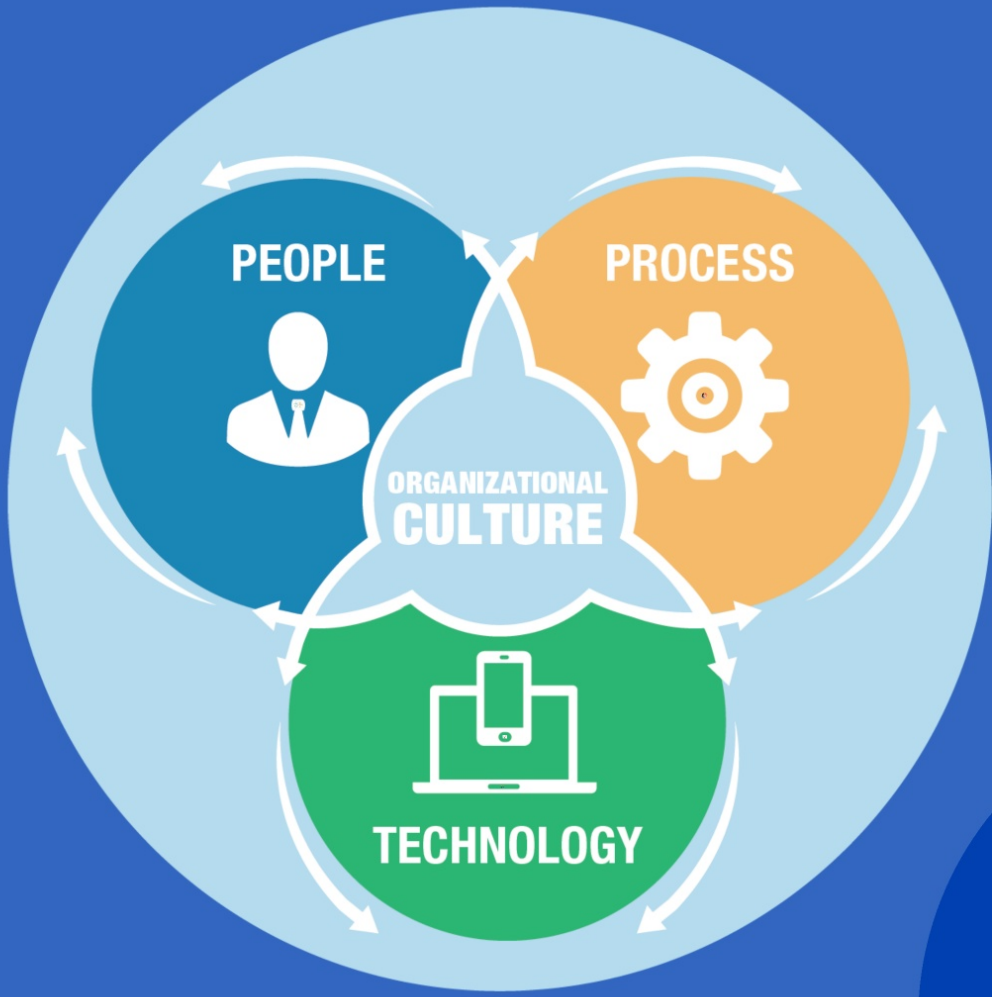
Security Operation Center

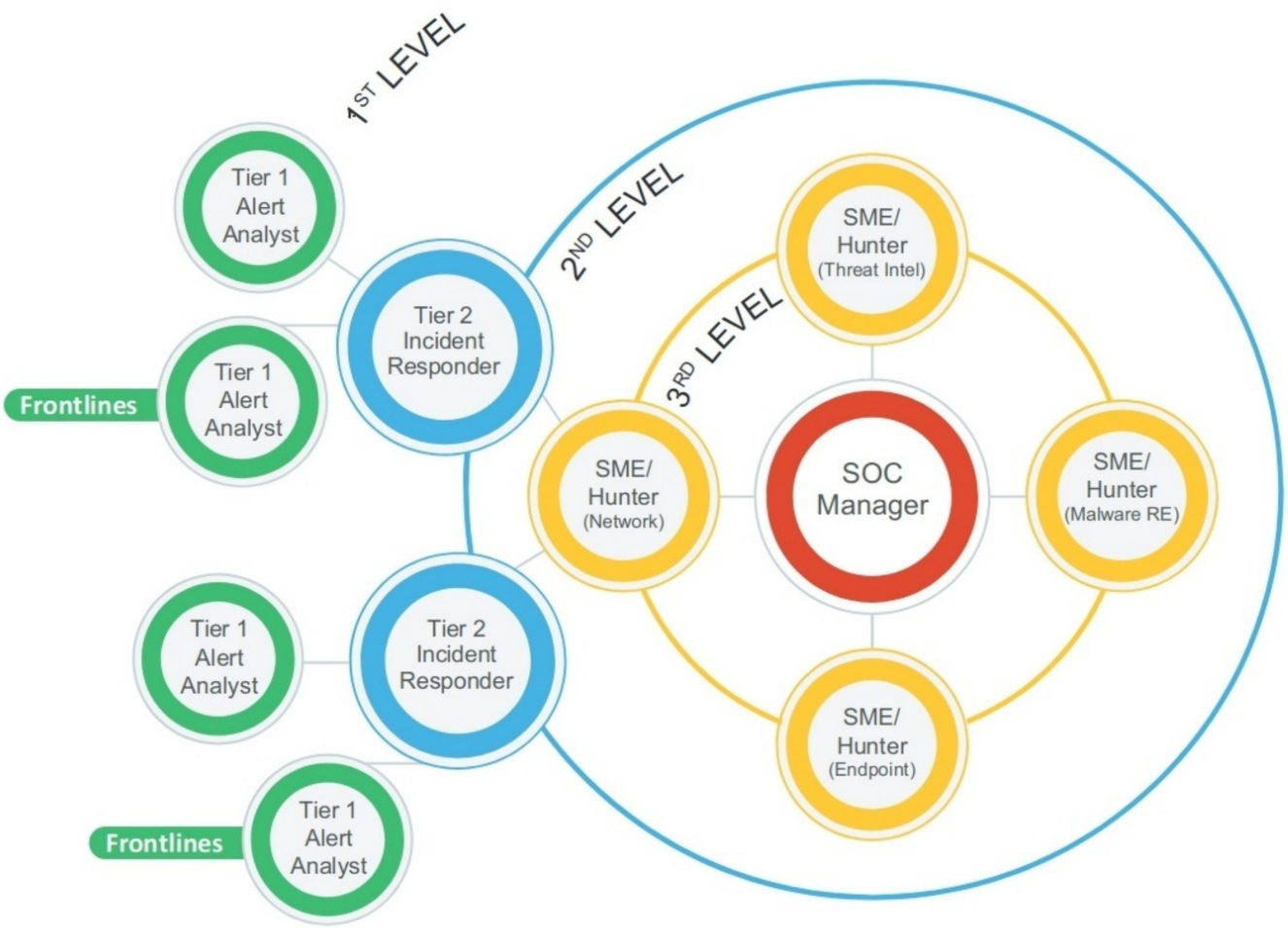
PPT modell



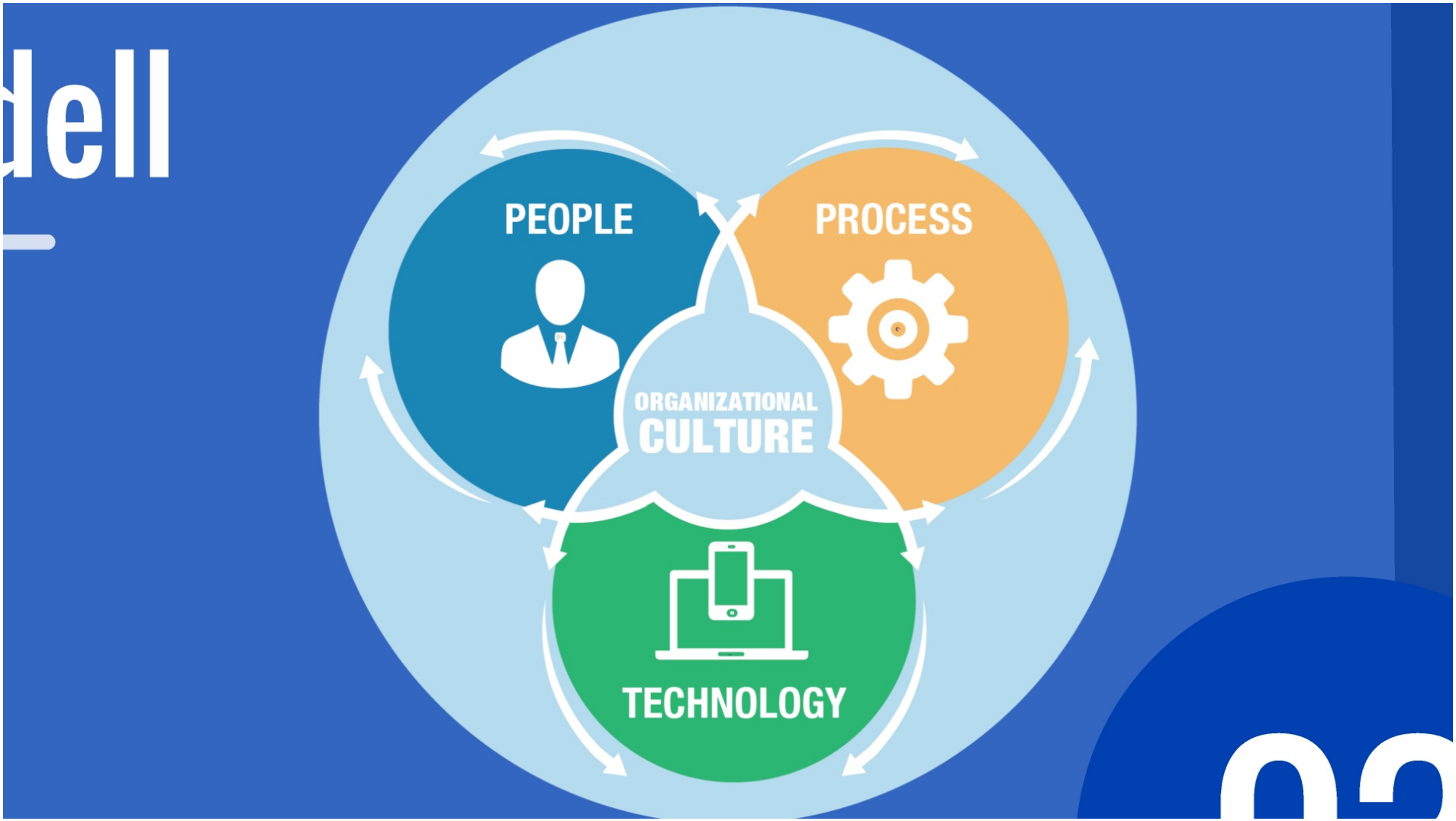
03

PPT modell




1ST LEVEL
2ND LEVEL
3RD LEVEL
Tier 1 Alert Analyst
Tier 1 Alert Analyst
Frontlines
Tier 2 Incident Responder
Tier 1 Alert Analyst
Tier 1 Alert Analyst
Frontlines
Tier 2 Incident Responder
SME/ Hunter (Threat Intel)
SME/ Hunter (Network)
SOC Manager
SME/ Hunter (Malware RE)
SME/ Hunter (Endpoint)

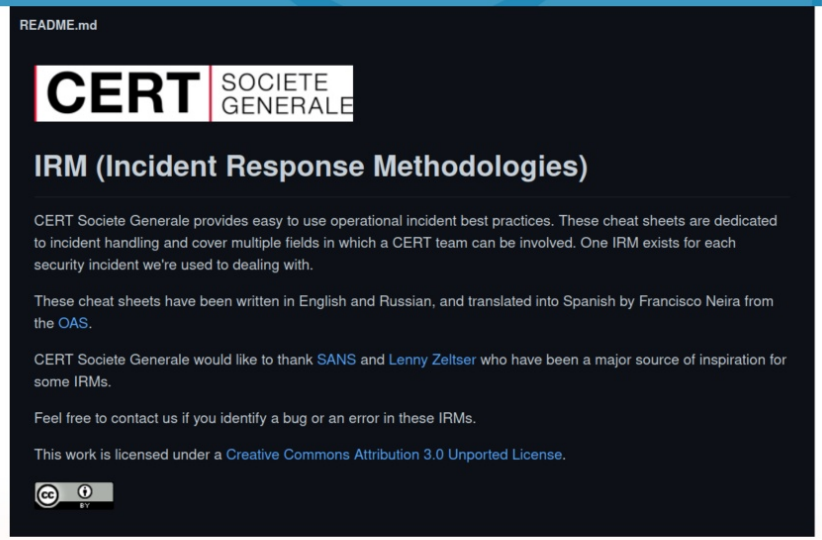

esa
esoc
esa
esoc
european space operations centre


PEOPLE
PROCESS
ORGANIZATIONAL
CULTURE
TECHNOLOGY


Prepare
Detect
Contain
Remediate
Communicate
Learn
Effective
Incident
Management

INTRODUCING THE LATEST MODULE IN
CISA'S CYBER SECURITY EVALUATION TOOL:

RANSOMWARE READINESS ASSESSMENT



Tisztelt Partnereink!

Mint korábban már jeleztük, informatikai rendszerünket egy zsaroló csoport vírussal támadta meg.

A támadás egy jól előkészített, alaposan megtervezett művelet volt. Az eddig fellelt nyomok alapján hetekig készülhettek rá a támadók. Sajnos rendszereink nagyon mélyen sérültek, a pusztítás gyakorlatilag totális volt, de mivel mentéseink rendelkezésre álltak, így újra tudtuk építeni a rendszert. Az elmúlt napokban saját szakembereink és külsős kollégák megfeszített, emberfeletti munkával éjjel-nappal dolgozva újjáépítették informatikai rendszerünket, teljesen az alapoktól. Sokan napokig nem mentek haza, és az ünnepeket is együtt töltöttük bent az informatikai központunkban. De ugyanígy keményen dolgoztak a kirendeltségeinken is kollégáink a helyi számítógépeken. Ezúton is szeretnénk megköszönni áldozatos munkájukat, melynek eredményeként alap szolgáltatásaink újból működnek, és vásárlóinkat a megszokott módon tudjuk kiszolgálni az UNIX TradeLine rendszeren keresztül.

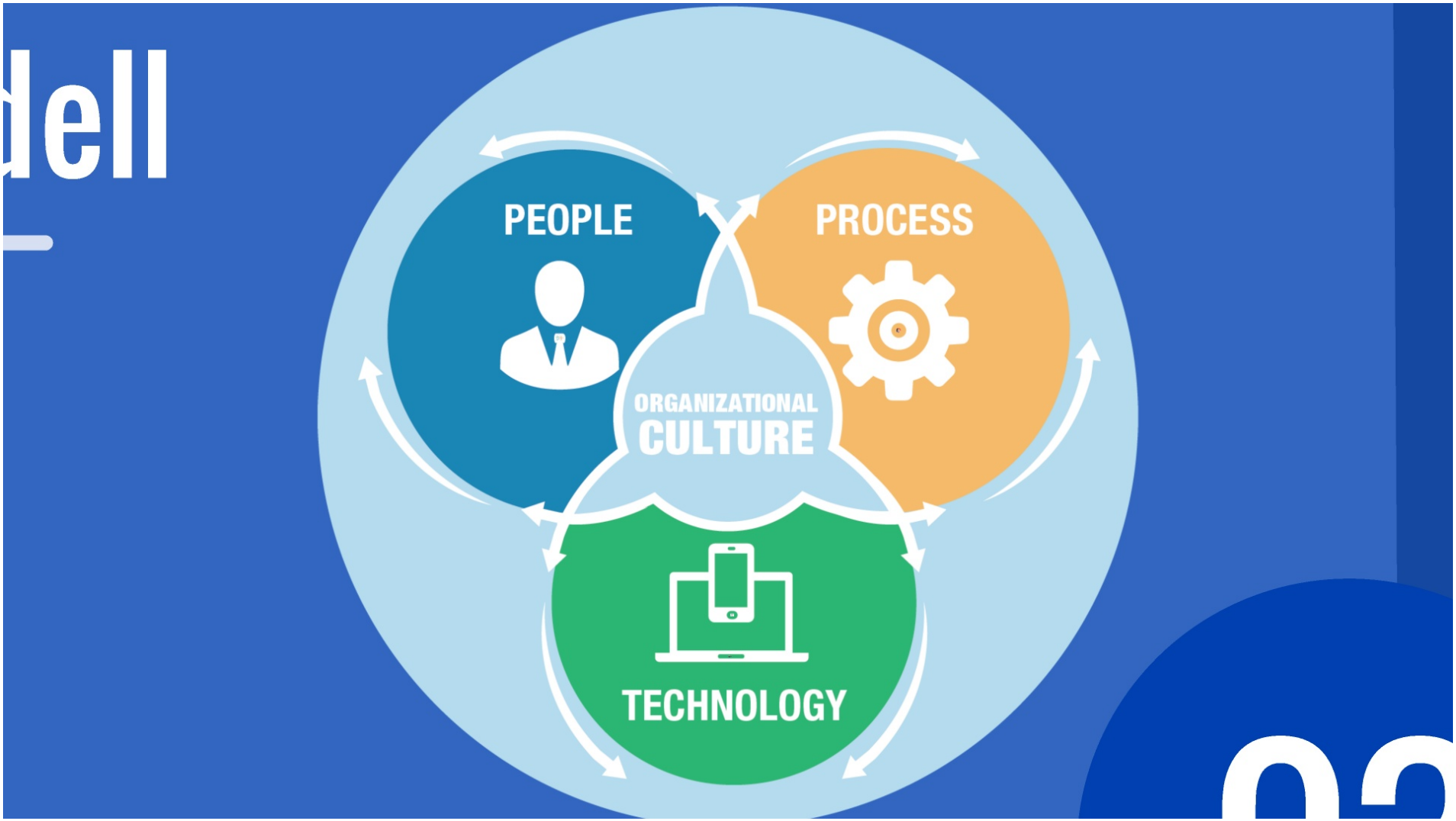
A helyreállítás után az adatveszteségünk végül mindössze a támadás előtti utolsó 12 perc adatai. Ezért az utolsó 12 percben beérkezett rendeléseket sajnos már nem tudjuk teljesíteni, ezért elnézést kérünk.

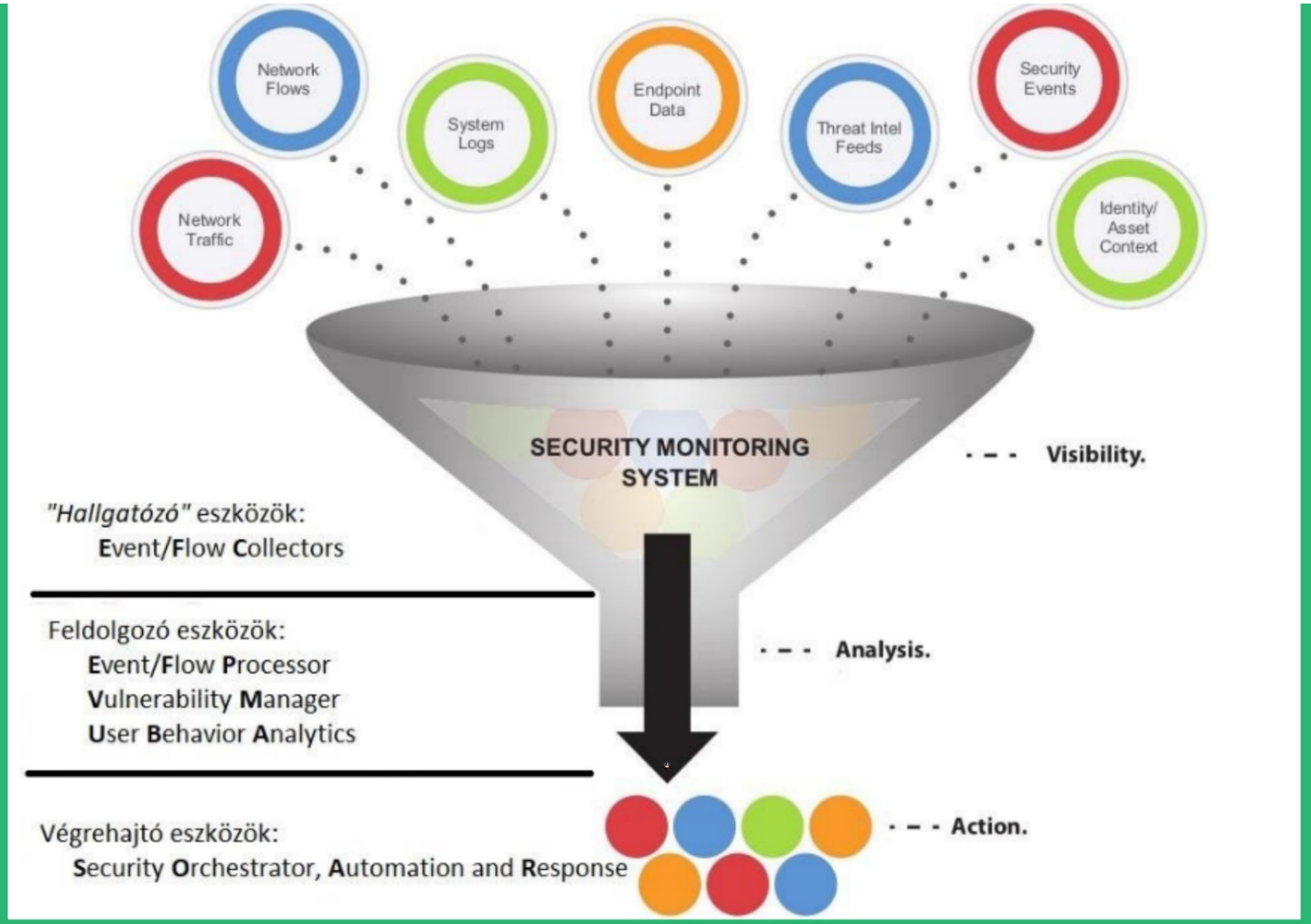
Néhány kiegészítő rendszer helyreállítása még folyamatban van, ezeket munkaidőn kívül végzik kollégáink, így az éjszakai órákban rendszerünk nem lesz elérhető. Weboldalunk helyreállítás még szintén folyamatban van, a webshop a hét második felében lesz újra aktív.

Azt sajnos tudni kell, a zsarolók gyakorlatából kiindulva komoly esélye van, hogy újabb támadás éri cégünket. Mi a legjobb tudásunk szerint felkészültünk és megfelelő védelmi rendszereket alakítottunk ki, de természetesen előfordulhat, hogy újabb támadás esetén a védekezés miatt szolgáltatásainkat átmenetileg újra korlátoznunk kell. Ezért előre is elnézésüket kérjük.

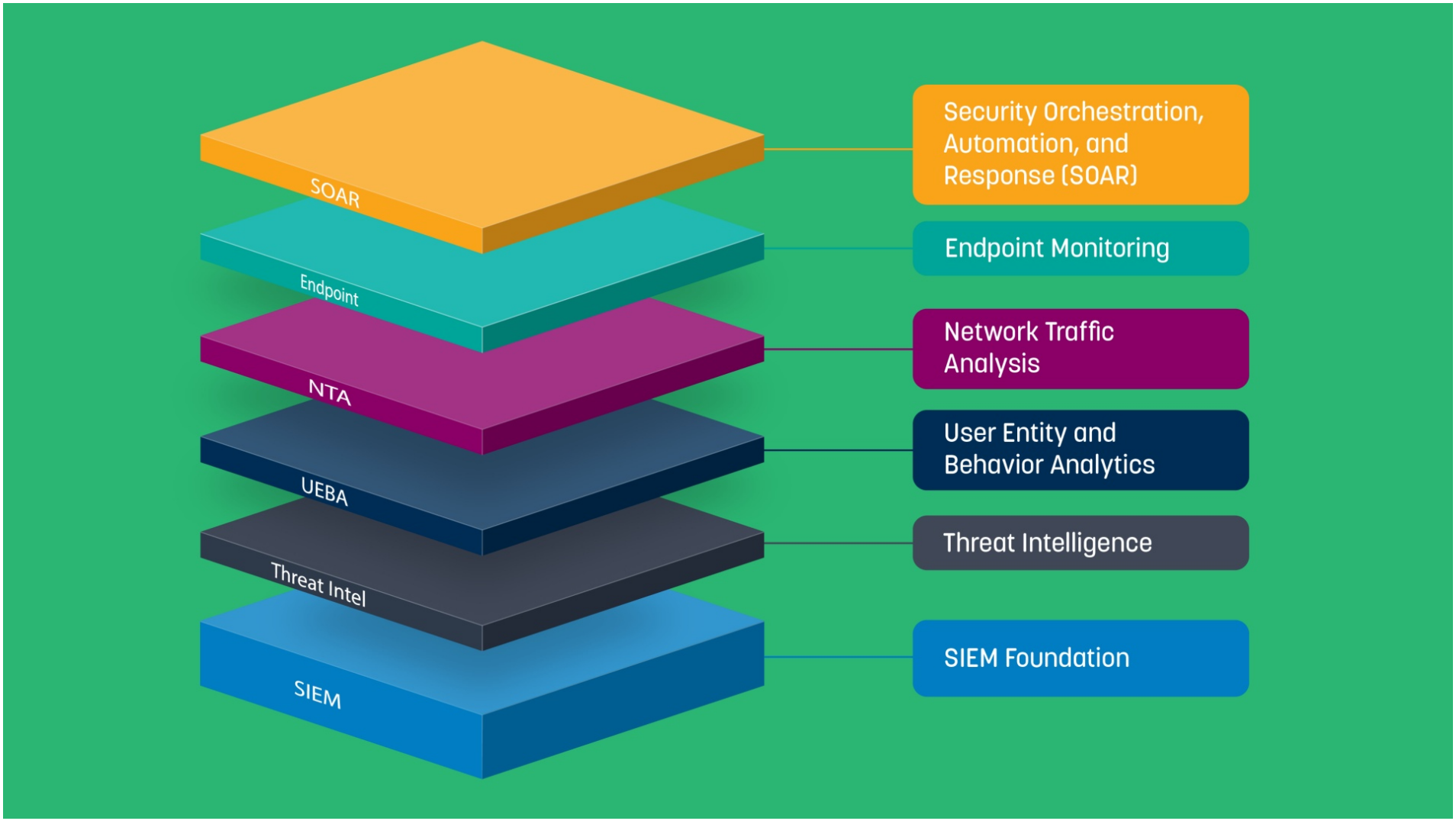
Nagyon köszönjük türelmüket, megértésüket, és azoknak, akik az elmúlt napokban nekünk szurkoltak, külön köszönetet szeretnénk mondani.

Zomberi Antal és az UNIX Csapata


PEOPLE
PROCESS
ORGANIZATIONAL
CULTURE
TECHNOLOGY


Network Flows
System Logs
Endpoint Data
Threat Intel Feeds
Security Events
Network Traffic
Identity/ Asset Context
SECURITY MONITORING SYSTEM
- – - Visibility.
"Hallgatózó" eszközök:
Event/Flow Collectors
Feldolgozó eszközök:
Event/Flow Processor
Vulnerability Manager
User Behavior Analytics
- – - Analysis.
Végrehajtó eszközök:
Security Orchestrator, Automation and Response
- – - Action.


Hack és lángos
HnL VIP 0014 - Állásinterjú

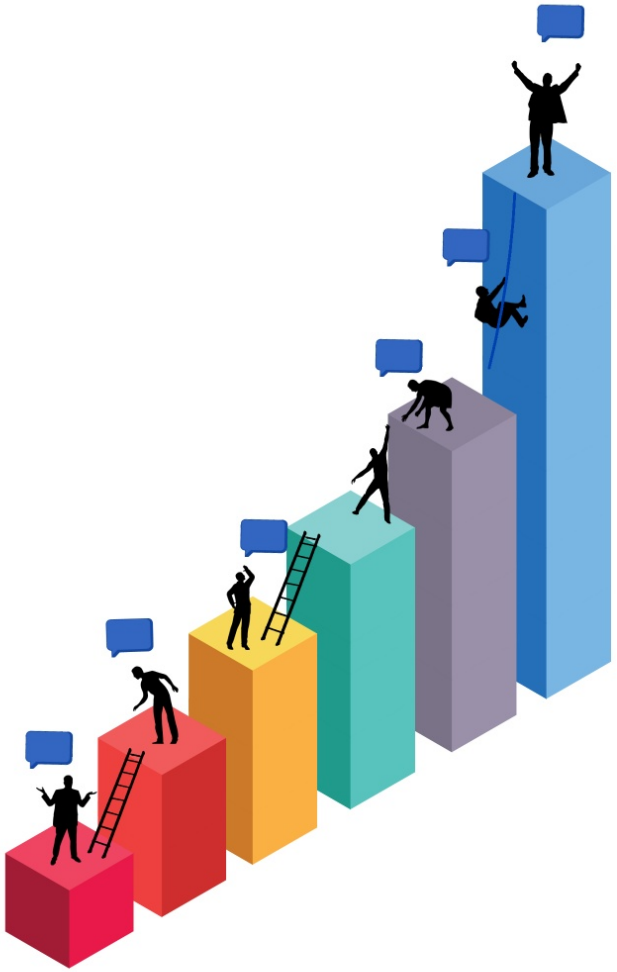

SOAR
Endpoint
NTA
UEBA
Threat Intel
SIEM
Security Orchestration, Automation, and Response (SOAR)
Endpoint Monitoring
Network Traffic Analysis
User Entity and Behavior Analytics
Threat Intelligence
SIEM Foundation

Rögzítendő jó

SOCaaS OK

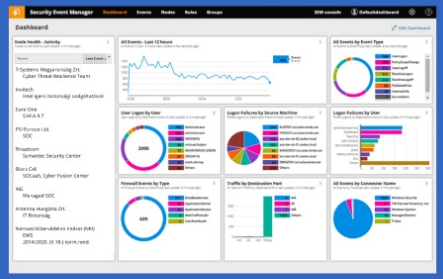
avagy jó gyakorlatok kiberbiztonsági központokban

Ötvös Antal - CISSP, ISO 27001 CLA

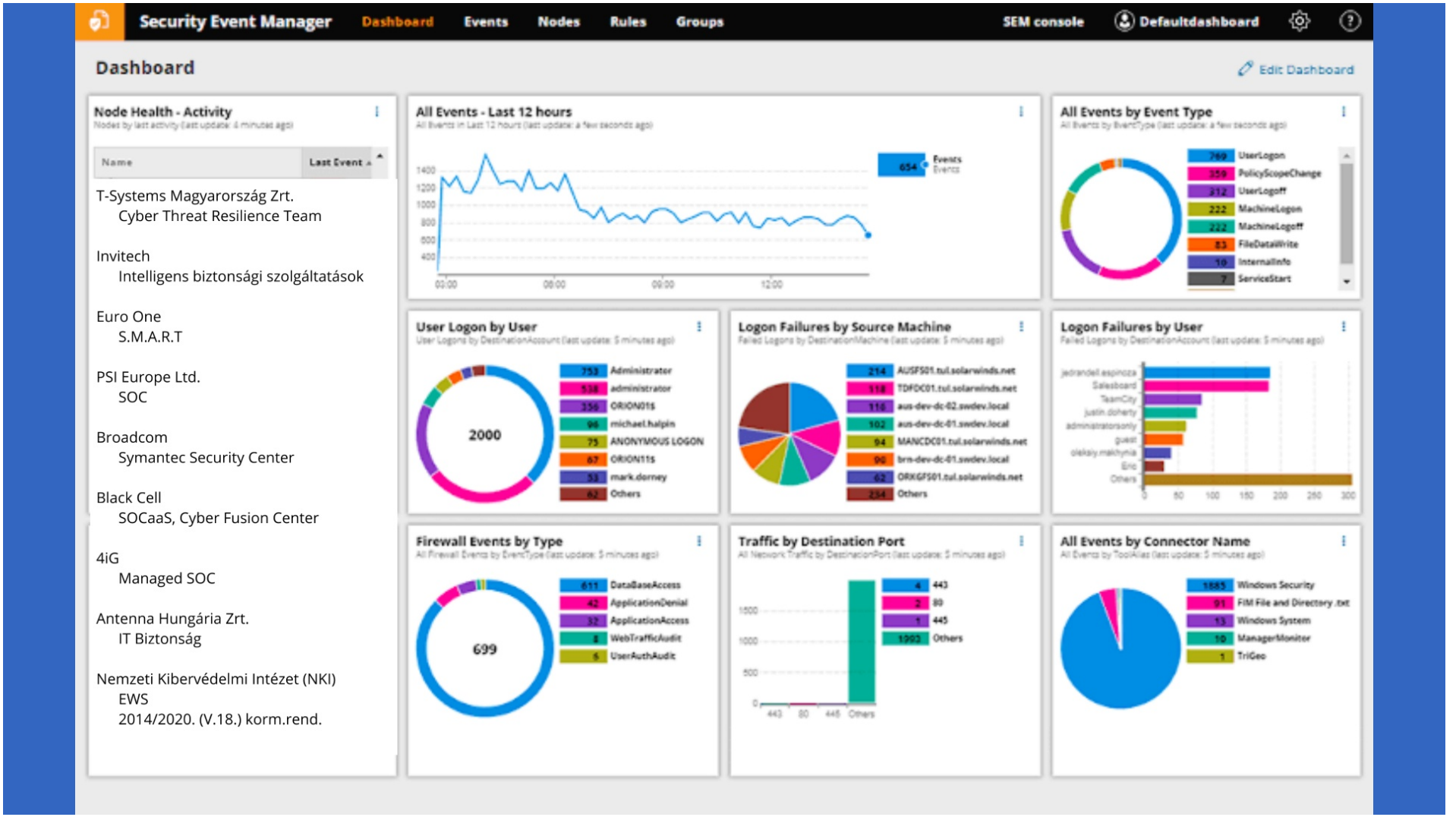


Körkép

Magyarország - Versenyszféra



04


Security Event Manager
Dashboard
Events
Nodes
Rules
Groups
SEM console
Defaultdashboard
Dashboard
Edit Dashboard
Node Health - Activity
Nodes by last activity (last update: 4 minutes ago)
Name
Last Event
T-Systems Magyarország Zrt.
Cyber Threat Resilience Team
Invitech
Intelligens biztonsági szolgáltatások
Euro One
S.M.A.R.T
PSI Europe Ltd.
SOC
Broadcom
Symantec Security Center
Black Cell
SOCaaS, Cyber Fusion Center
4iG
Managed SOC
Antenna Hungária Zrt.
IT Biztonság
Nemzeti Kibervédelmi Intézet (NKI)
EWS
2014/2020. (V.18.) korm.rend.
All Events - Last 12 hours
All Events in Last 12 hours (last update: a few seconds ago)
654
Events
All Events by Event Type
All Events by EventType (last update: a few seconds ago)
769 UserLogon
359 PolicyScopeChange
312 UserLogoff
222 MachineLogon
222 MachineLogoff
83 FileDataWrite
10 InternalInfo
7 ServiceStart
User Logon by User
User Logons by DestinationAccount (last update: 5 minutes ago)
2000
753 Administrator
538 administrator
356 ORION01$
96 michael.halpin
75 ANONYMOUS LOGON
67 ORION11$
53 mark.dorney
62 Others
Logon Failures by Source Machine
Failed Logons by DestinationMachine (last update: 5 minutes ago)
214 AUSFS01.tul.solarwinds.net
118 TDFDC01.tul.solarwinds.net
116 aus-dev-dc-02.swdev.local
102 aus-dev-dc-01.swdev.local
94 MANCDC01.tul.solarwinds.net
90 brn-dev-dc-01.swdev.local
62 ORKGFS01.tul.solarwinds.net
234 Others
Logon Failures by User
Failed Logons by DestinationAccount (last update: 5 minutes ago)
jedrandell.espinoza
Salesboard
TeamCity
justin.doherty
administratorsonly
guest
oleksiy.makhynia
Eric
Others
0
50
100
150
200
250
300
Firewall Events by Type
All Firewall Events by EventType (last update: 5 minutes ago)
699
611 DataBaseAccess
42 ApplicationDenial
32 ApplicationAccess
8 WebTrafficAudit
6 UserAuthAudit
Traffic by Destination Port
All Network Traffic by DestinationPort (last update: 5 minutes ago)
1500
1000
500
0
443
80
445
Others
4 443
2 80
1 445
1903 Others
All Events by Connector Name
All Events by ToolAlias (last update: 5 minutes ago)
1885 Windows Security
91 FIM File and Directory .txt
13 Windows System
10 ManagerMoniter
1 TriGeo

T-Systems Magyarország Zrt.
Cyber Threat Resilience Team

Invitech
Intelligens biztonsági szolgáltatások

Euro One
S.M.A.R.T

PSI Europe Ltd.
SOC

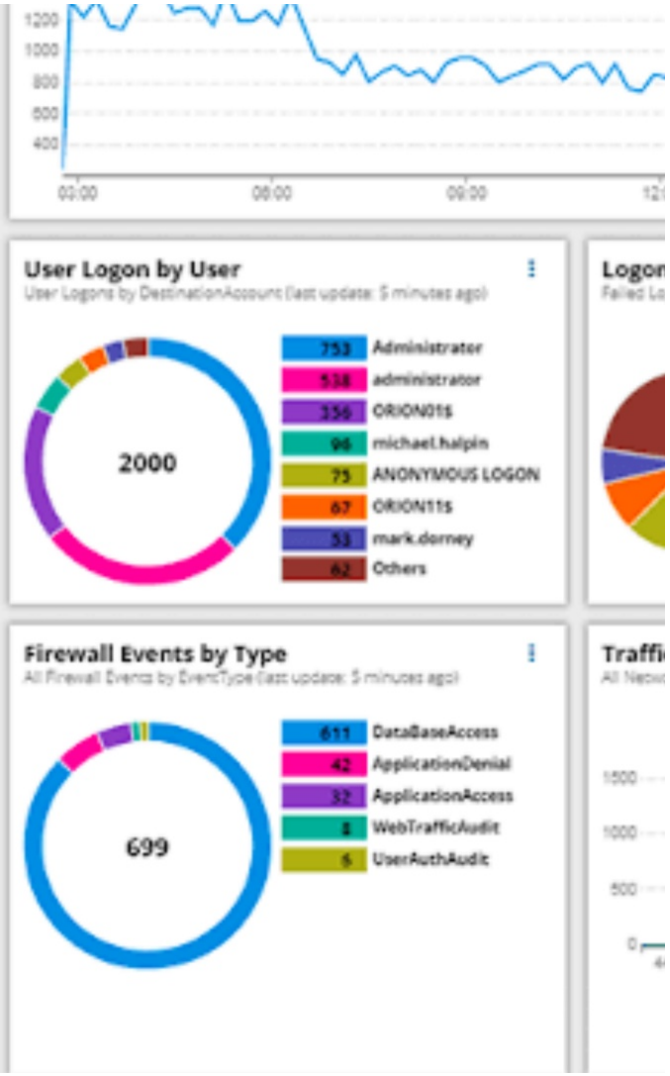
Broadcom
Symantec Security Center

Black Cell
SOCaaS, Cyber Fusion Center

4iG
Managed SOC

Antenna Hungária Zrt.
IT Biztonság

Nemzeti Kibervédelmi Intézet (NKI)
EWS
2014/2020. (V.18.) korm.rend.

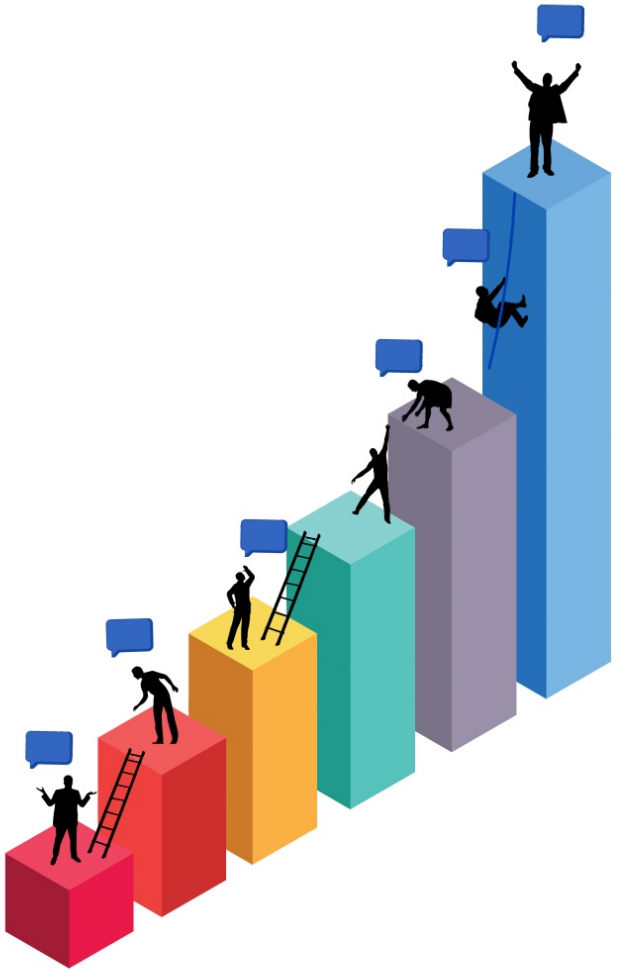


Rögzítendő jó

SOCaaS OK

avagy jó gyakorlatok
kiberbiztonsági központokban

Ötvös Antal - CISSP, ISO 27001 CLA



Jó SOCaaS OK

05

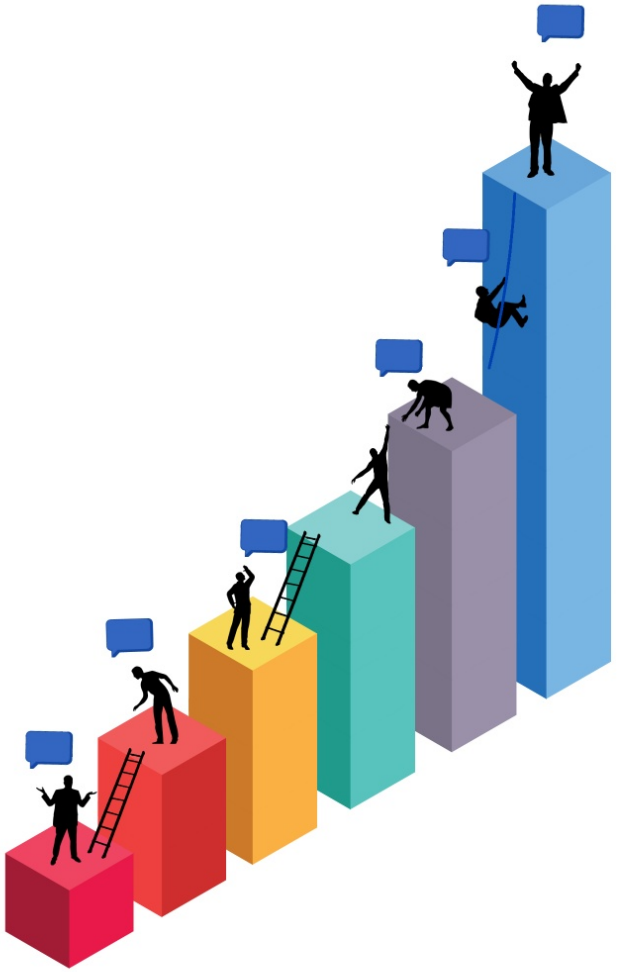

7 KPIs
6 Minősítés
5 Automatizálás
4 Incidens menedzsment
3 Struktúra kialakítása
2 Stratégia alkotás
1 Vezetői elköteleződés

Rögzítendő jó

SOCaaS OK

avagy jó gyakorlatok
kiberbiztonsági központokban

Ötvös Antal - CISSP, ISO 27001 CLA



Köszönöm a figyelmet!
Kérdések és válaszok

Hivatkozások

06

U.S. Department of Defense
https://www.defense.gov/News/Releases/Release/Article/2079489/dod-releases-fiscal-year-2021-budget-proposal/

Ludovika Szabadegyetem - Dr. Kovács László dandártábornok (2022.03.08.)
https://www.youtube.com/watch?v=EVWBlB6rK-M&t=7s

European Space Agency
https://www.esa.int/Enabling_Support/Operations/Replay_Mars_Express_tracking_NASA_Mars_landing

SANS – Building a Word Class Security Operation Center
https://www.emc.com/collateral/white-papers/rsa-advanced-soc-solution-sans-soc-roadmap-white-paper.pdf

Enterprise Security Leadership: Creating a World Class Security Operations Center (SOC)
https://www.cybrary.it/course/enterprise-security-leadership-creating-a-world-class-security-operations/

NGS Infonet – SOC As A Service
https://ngsinfonet.com/soc-as-a-service.php

Köszönöm a figyelmet!
Kérdések és válaszok

Hivatkozások

06

Rögzítendő jó

SOCaaS OK

avagy jó gyakorlatok
kiberbiztonsági központokban

Ötvös Antal - CISSP, ISO 27001 CLA