ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Kiberbiztonsági kutatások egy „Security Operation Center” falain belül

A workshop programja:

1. Egyetemi SOC fejlesztése – kihívások egy SOC-ban
2. User and entity behavior analytics
3. Honeypotok optimalizálása – hogyan ejtsük át a támadókat?
4. Capture the flag!
5. Hack the Box!
6. Cyber Range – hogyan lőjünk a kibertérben?
7. Támadási gráfok alkalmazhatósága a SOC-ban
8. Autóban is elfér egy SOC?
9. 5G kiberbiztonság
10. AI - kihívások és lehetőségek a kibervédelemben - vendégelőadás: Aradi Zoltán, NKI
11. Leitold Ferenc: Elosztott fenyegetettség felmérés; Felhasználói biztonságtudatosság automatikus mérése

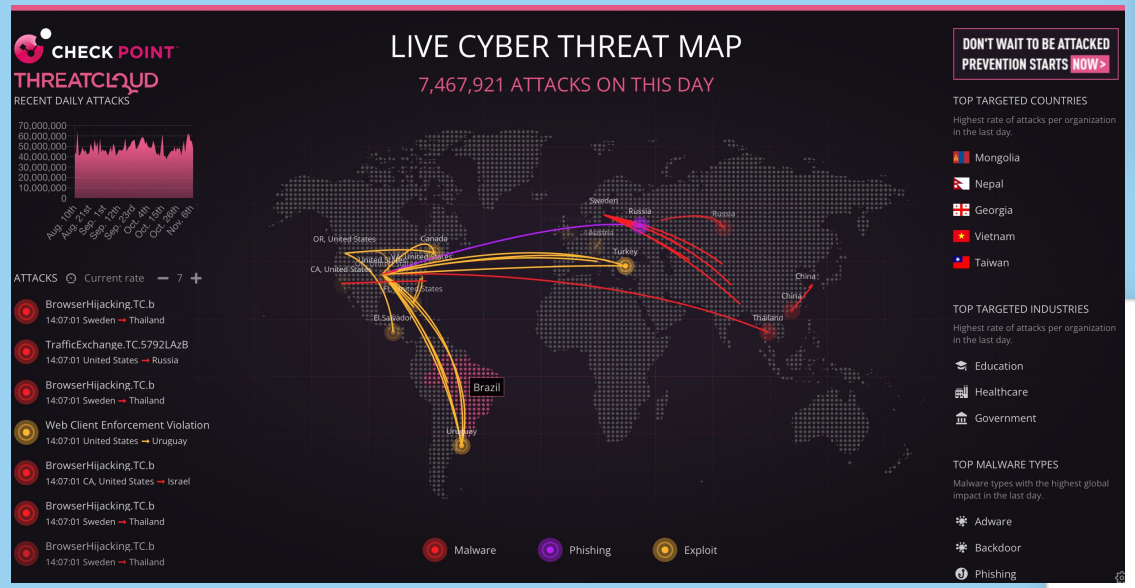
ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

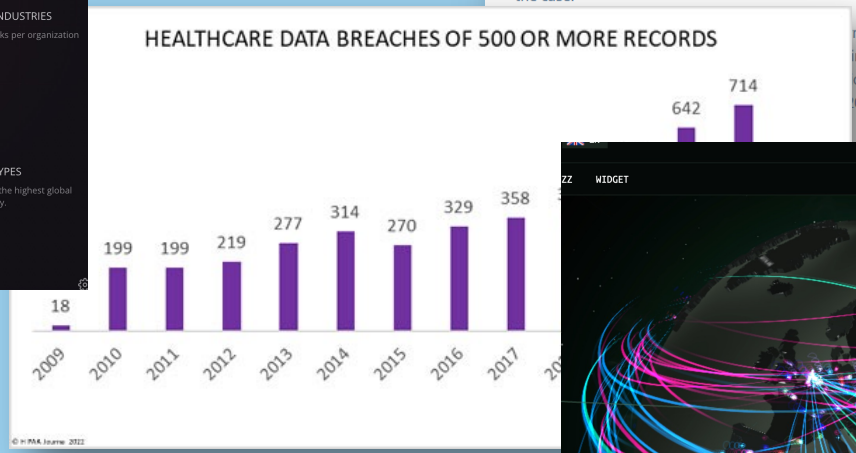
Security Operation Center

Dr. Bánáti Anna, ÓE NIK

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Támadók aktivitása





https://threatmap.checkpoint.com

https://cybermap.kaspersky.com/

https://www.cyberark.com/what-is/healthcare-cybersecurity/
https://www.hipaajournal.com/healthcare-data-breach-statistics/
https://www.theguardian.com/technology/2022/jul/14/ransomware-attacks-cybersecurity-targeting-us-hospitals
https://www.riskrecon.com

Hogyan védekezzünk? - Security Operation Center, SOC

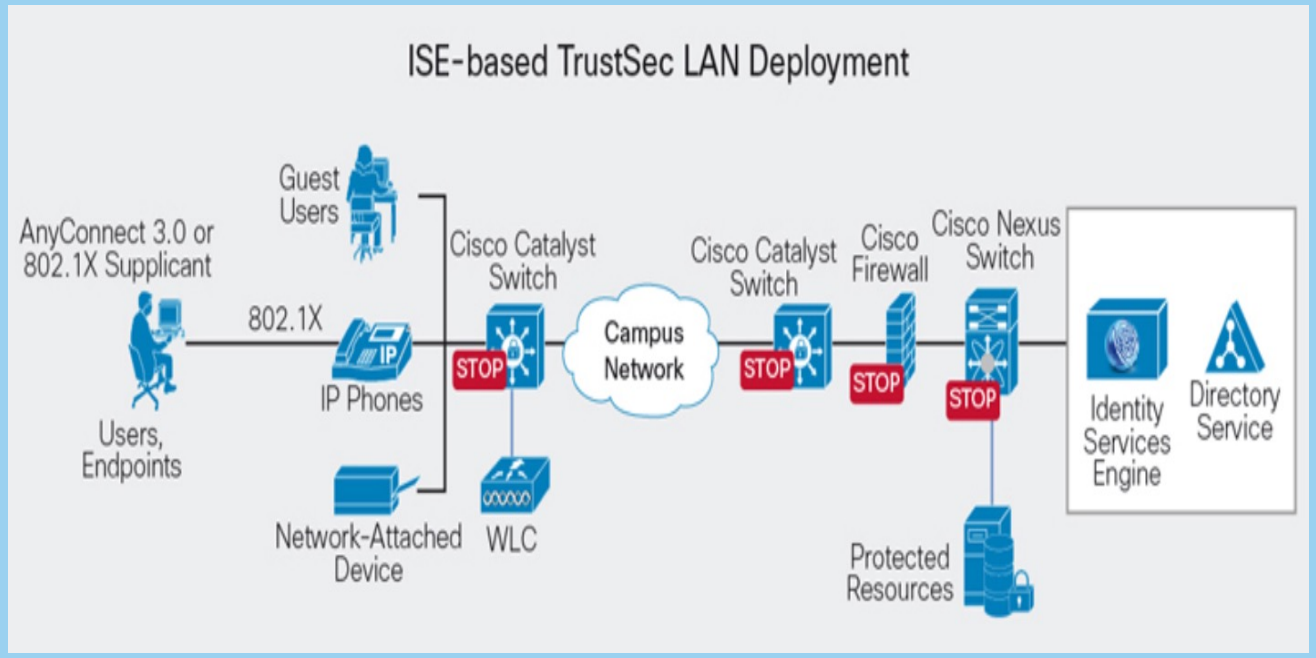
Hagyományos védelmi megoldások:

- Határvédelem
  - Tűzfal
  - IDS/IPS
  - Identity service
  - VPN

Modern védelmi megoldások:

- Átfogó védelem

SOC



https://www.routexp.com/2018/10/cisco-identity-services-engine-ise-user.html

Hogyan védekezzünk? - Security Operation Center, SOC

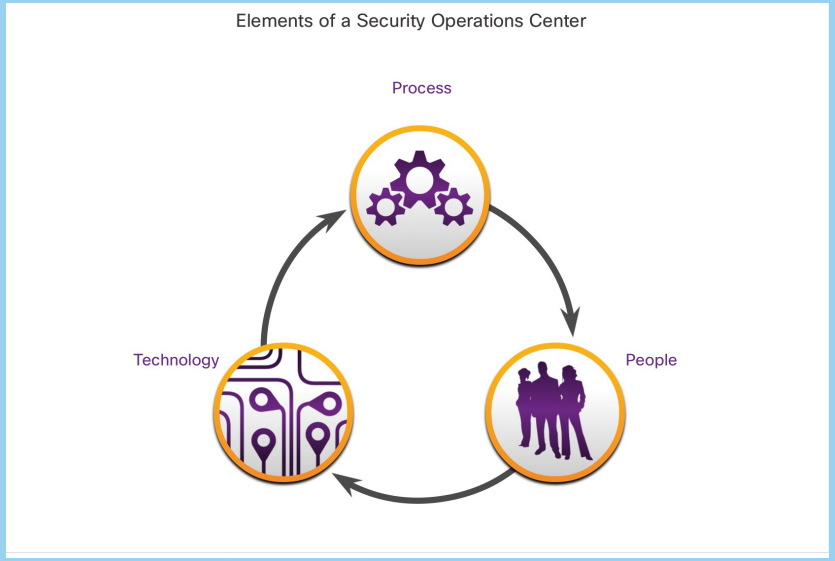
https://soc.uni-obuda.hu

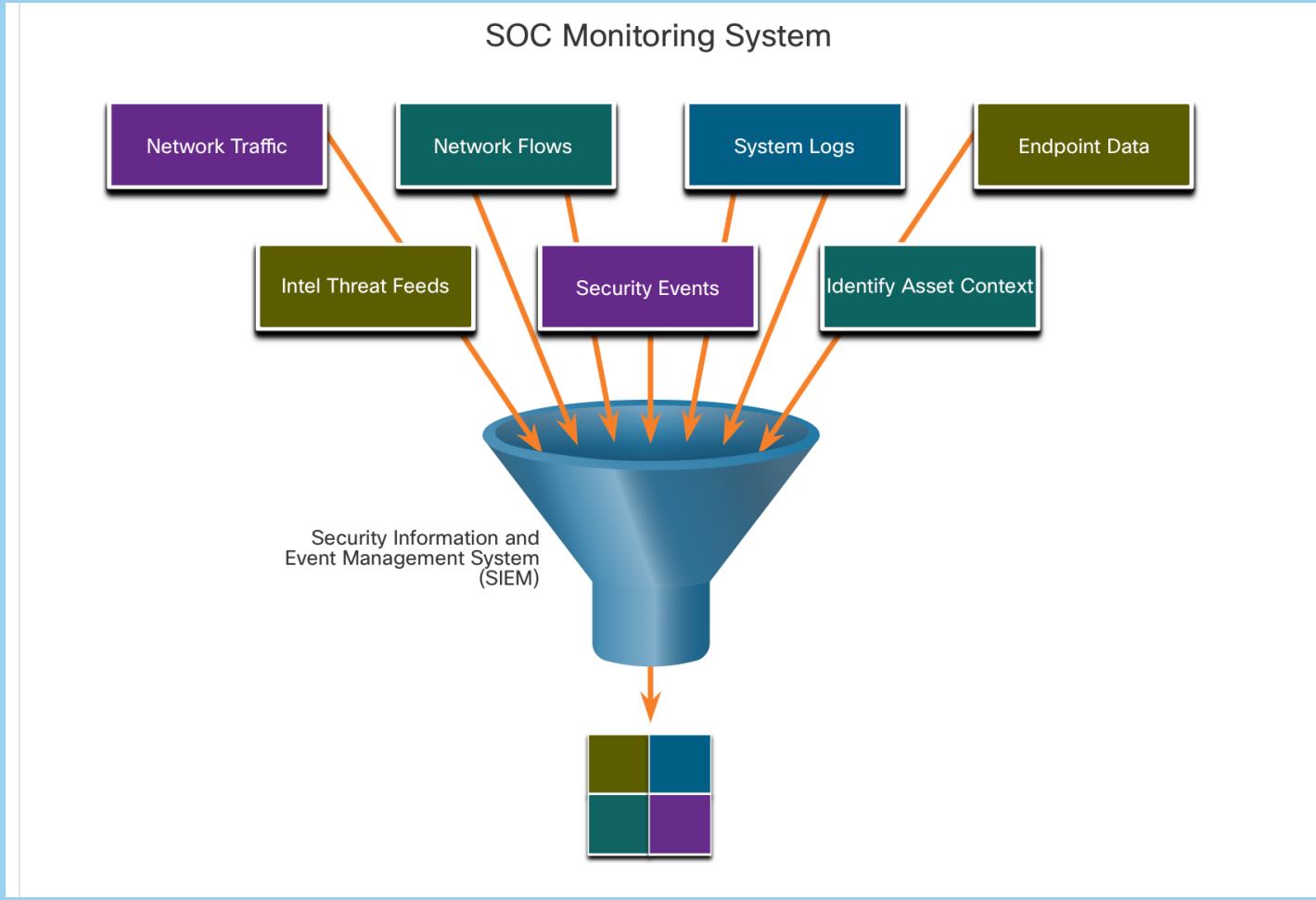
Hogyan védekezzünk? - Security Operation Center, SOC

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Security Operation Center, SOC

People	Process	Technology
SOC üzemeltető	Eszköz menedzsment	Monitorozó megoldások
Elemző	Változás menedzsment	Security Event Management
Incidens koordinátor	Incidens menedzsment	Sérülékenységvizsgálat
	Megfelelőségértékelés	Honeypot
		Tűzfal
		Behatolás detektáló



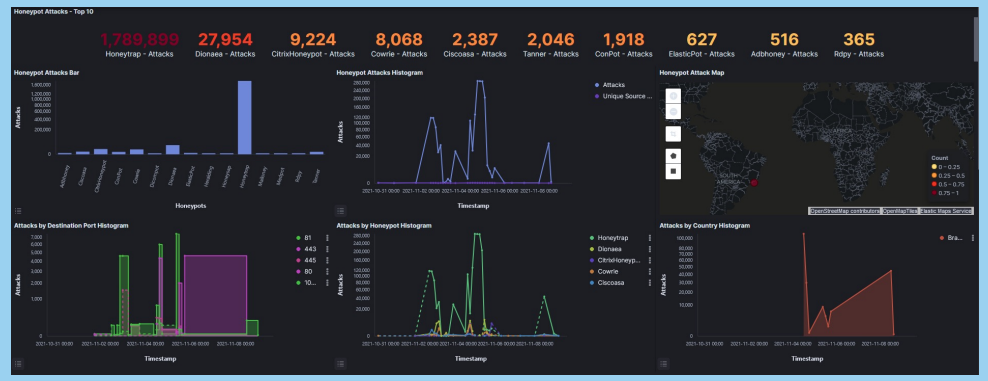


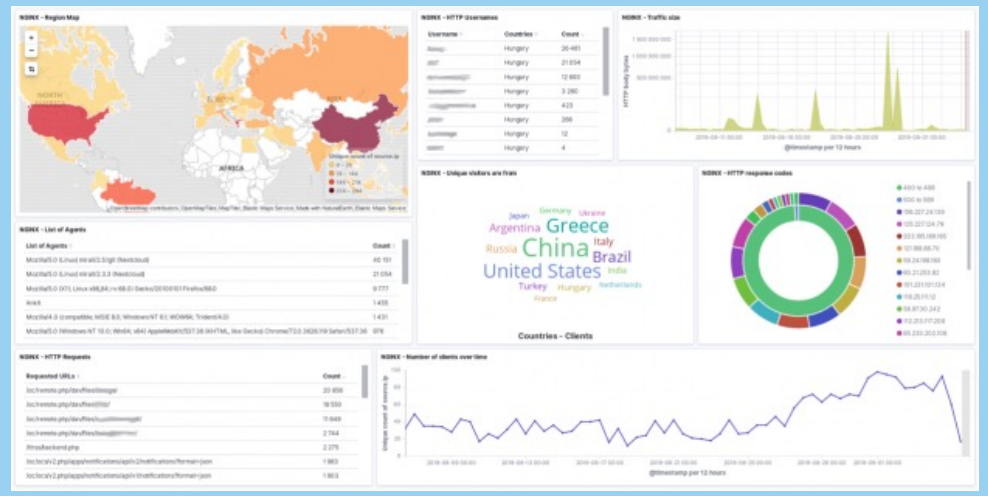
SECURITY OPERATION CENTER

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Feladatok:

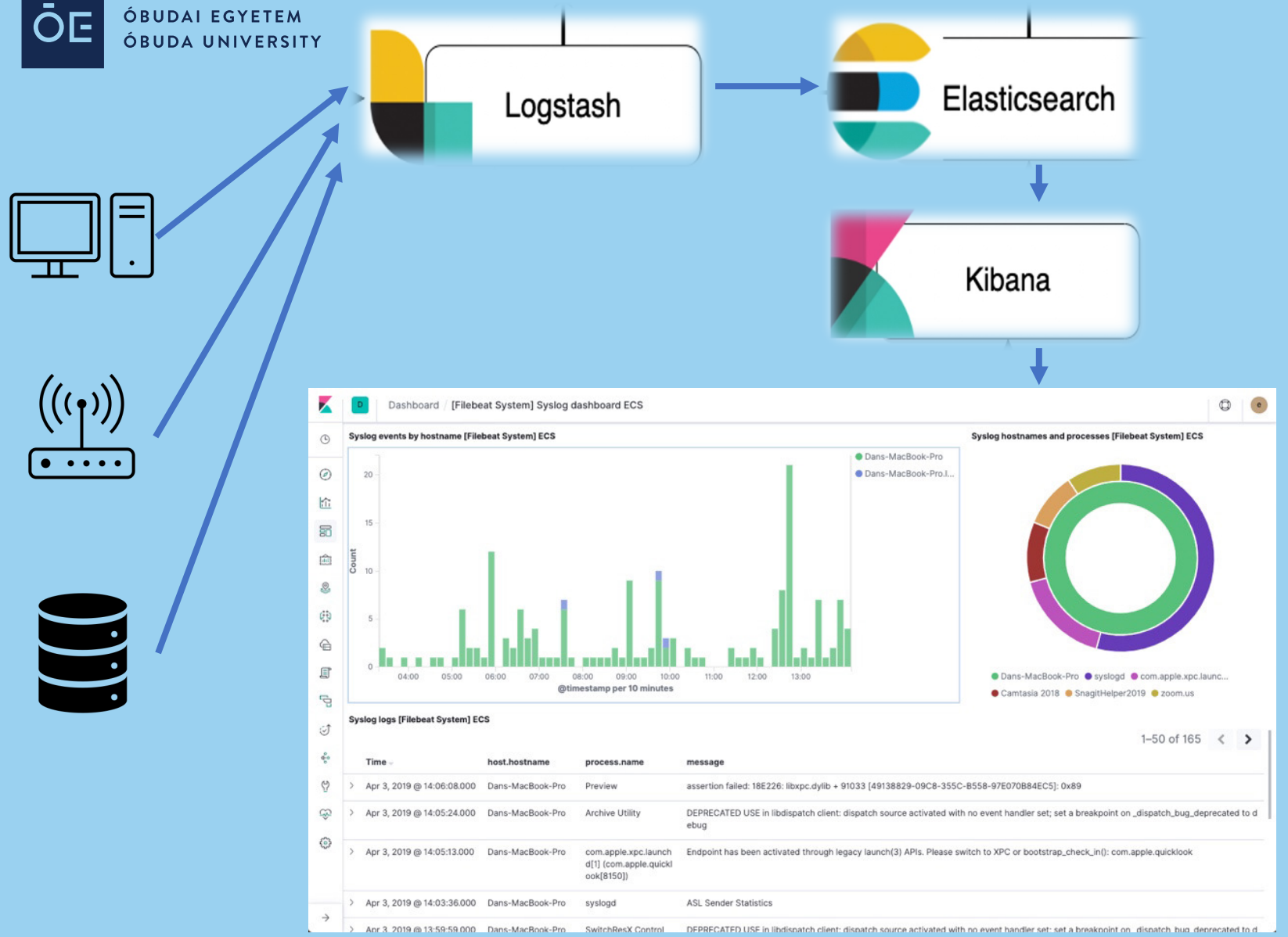
- Naplóadatok gyűjtése
- Naplóadatok elemzése
- Események korrelációja
- Riasztások definiálása
- Adatok vizualizálása
- Fehasználói adatok monitorozása





SECURITY INFORMATION and EVENT MANAGEMENT

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

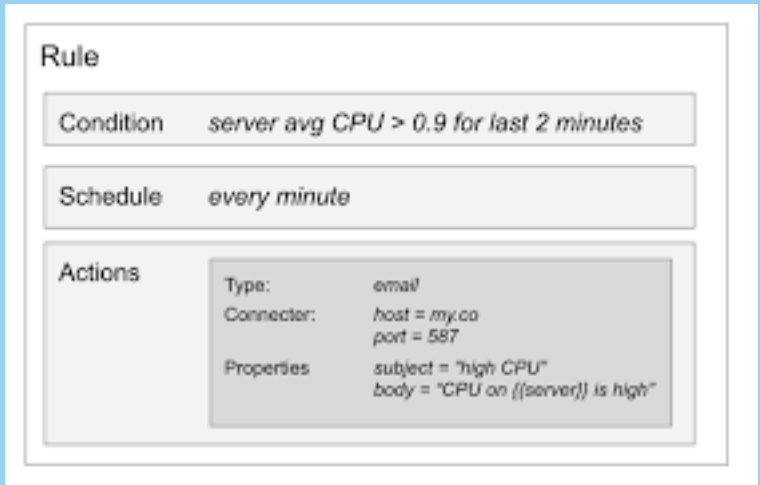


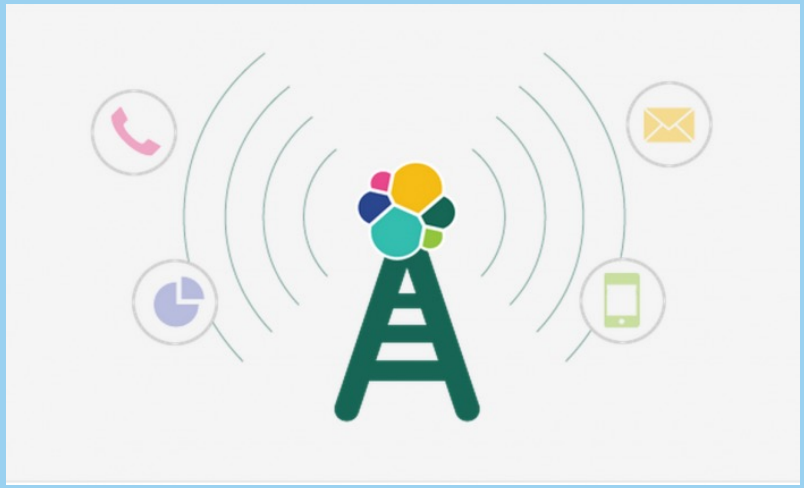
Elasticserach
Logstash
Kibana

Napló- és forgalmi adatok gyűjtése

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

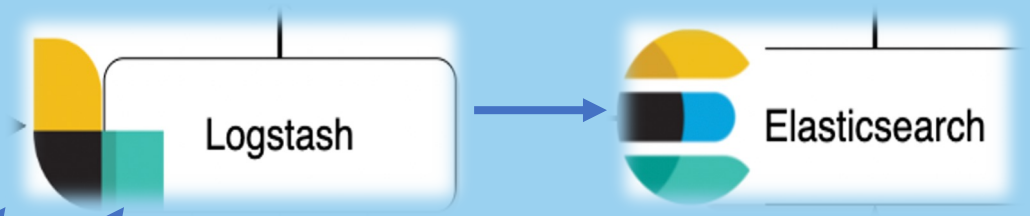
ALERTING

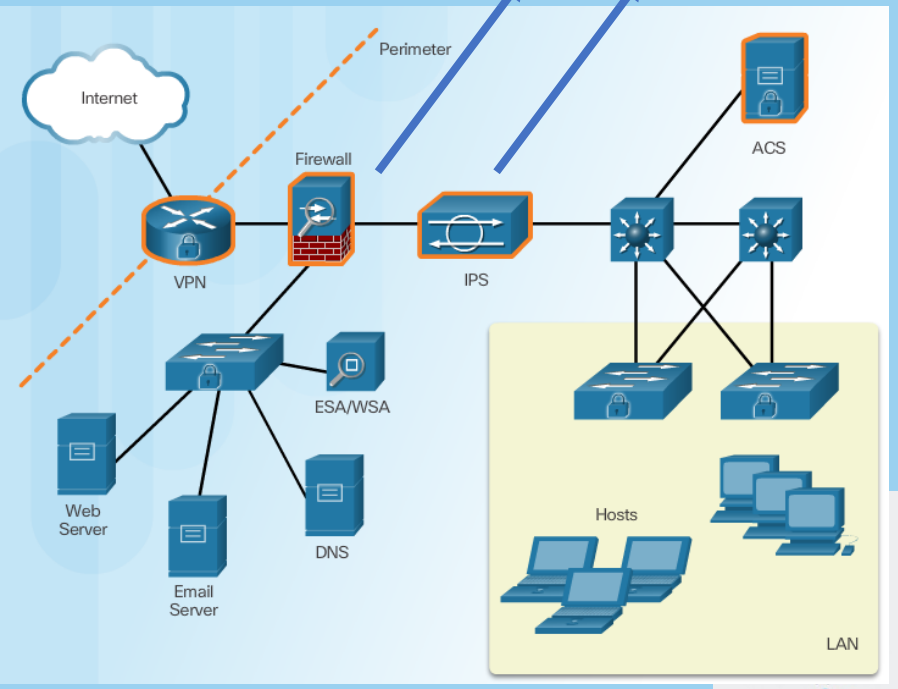


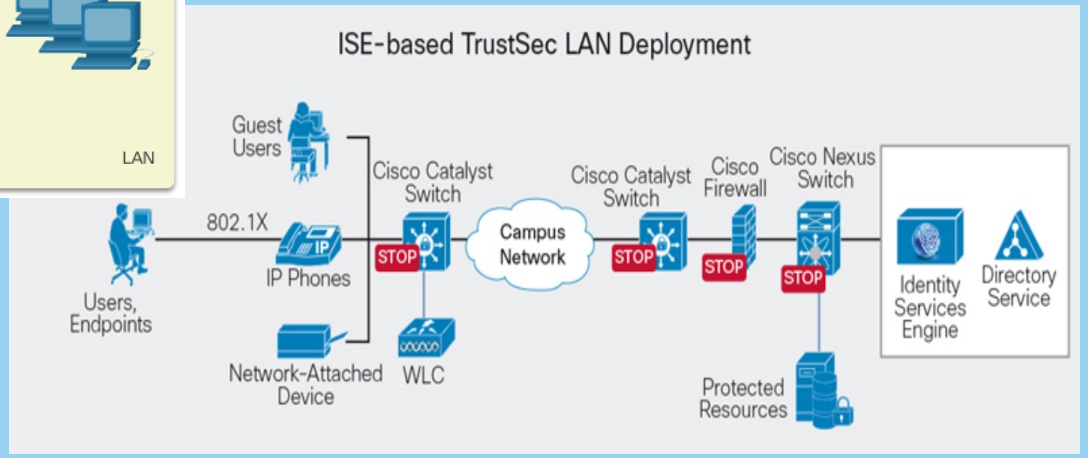


Alarm Type	Network Activity	IPS Activity	Outcome
False positive	Normal user traffic	Alarm generated	Tune alarm
False negative	Attack traffic	No alarm generated	Tune alarm
True positive	Attack traffic	Alarm generated	Ideal setting
True negative	Normal user traffic	No alarm generated	Ideal setting

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY



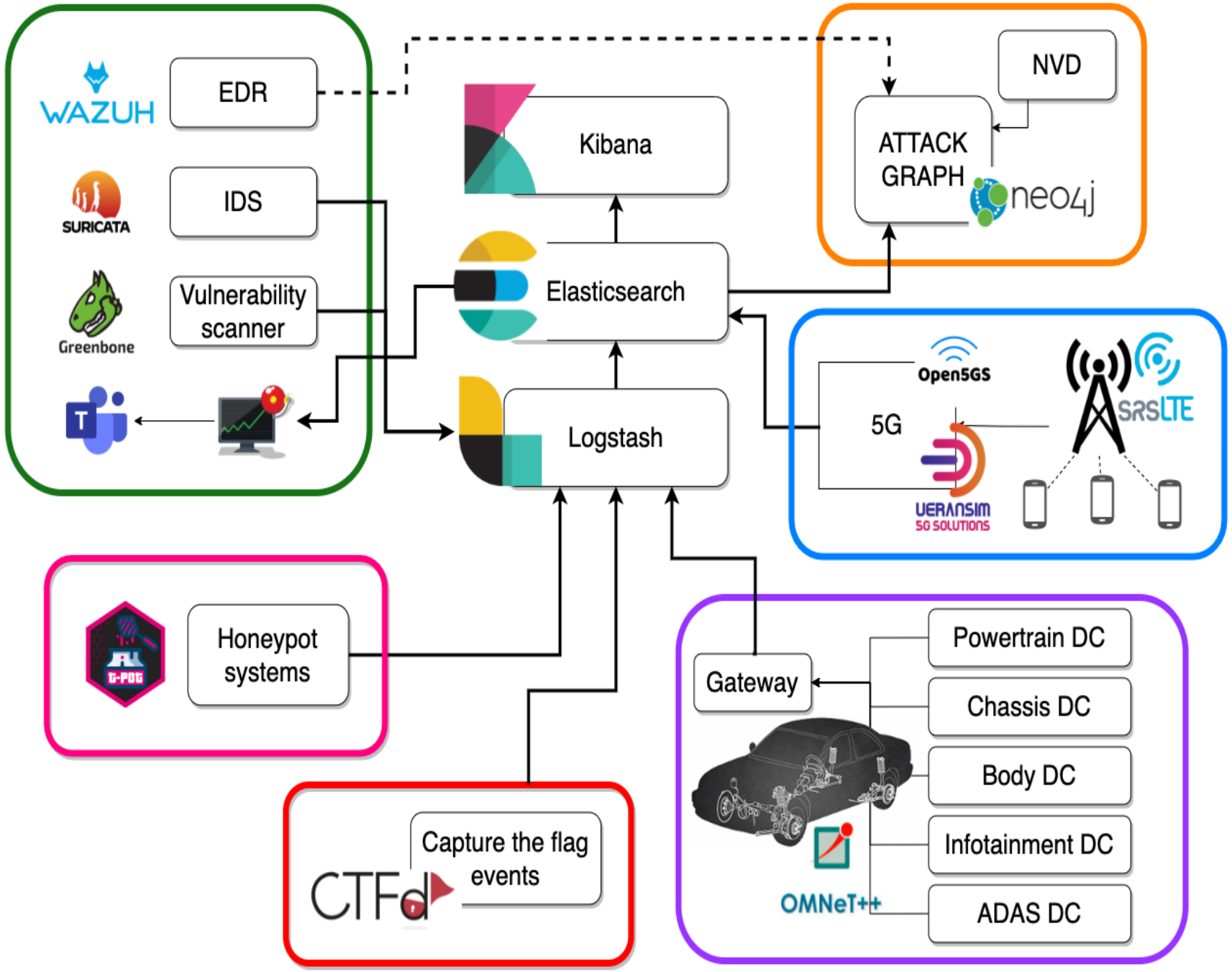




Bővítés:
IDS/IPS
HONEYPOT
FIREWALL

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Feladatok



NIK-SOC

HONEYPOT

CTF

ATTACK GRAPH

V-SOC

5G SOC

CYBER RANGE

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Kérdések:

Milyen komponenseket fejlesszünk tovább?

Hogyan optimalizáljuk a komponenseket?

Milyen események korrelációját vizsáljuk?

Miről állítsunk be riasztásokat?

Hogyan automatizáljuk az egyes folyamatokat?

Tagok:

- Érsok Máté
- Mohácsi Péter (Kiber)
- Szabó Szabolcs (Kiber)
- Aczél Juli (Msc)
- Kovács József (BSc)
- Párdi Imre (Kiber)
- Végvári Zsolt (MSc)
- Halaj Balázs (BSc)
- Páll Kristóf Soma (Kiber)

NIK-SOC

HONEYPOT

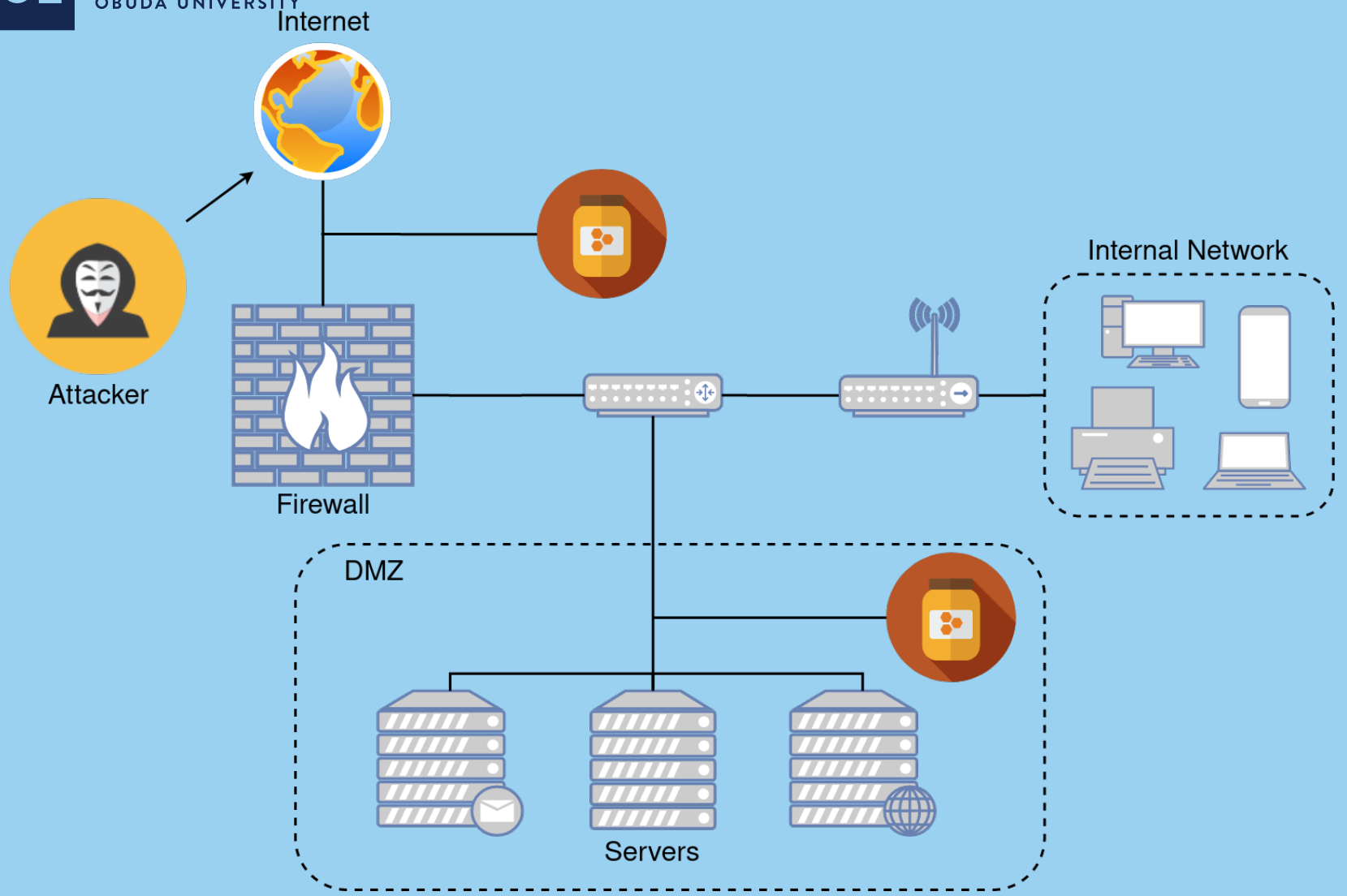
CTF

ATTACK GRAPH

V-SOC

5G SOC

CYBER RANGE



NIK-SOC
HONEYPOT
CTF
ATTACK GRAPH
V-SOC
5G SOC
CYBER RANGE

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Kérdések:

Milyen indikátorok mentén optimalizáljunk?

Hogyan profilozzuk a támadókat?

Hogyan álcázzuk a honeypotokat hatékonyan?

Hogyan dolgozzunk fel nagy mennyiségű “honypot-logokat”?

Tagok:

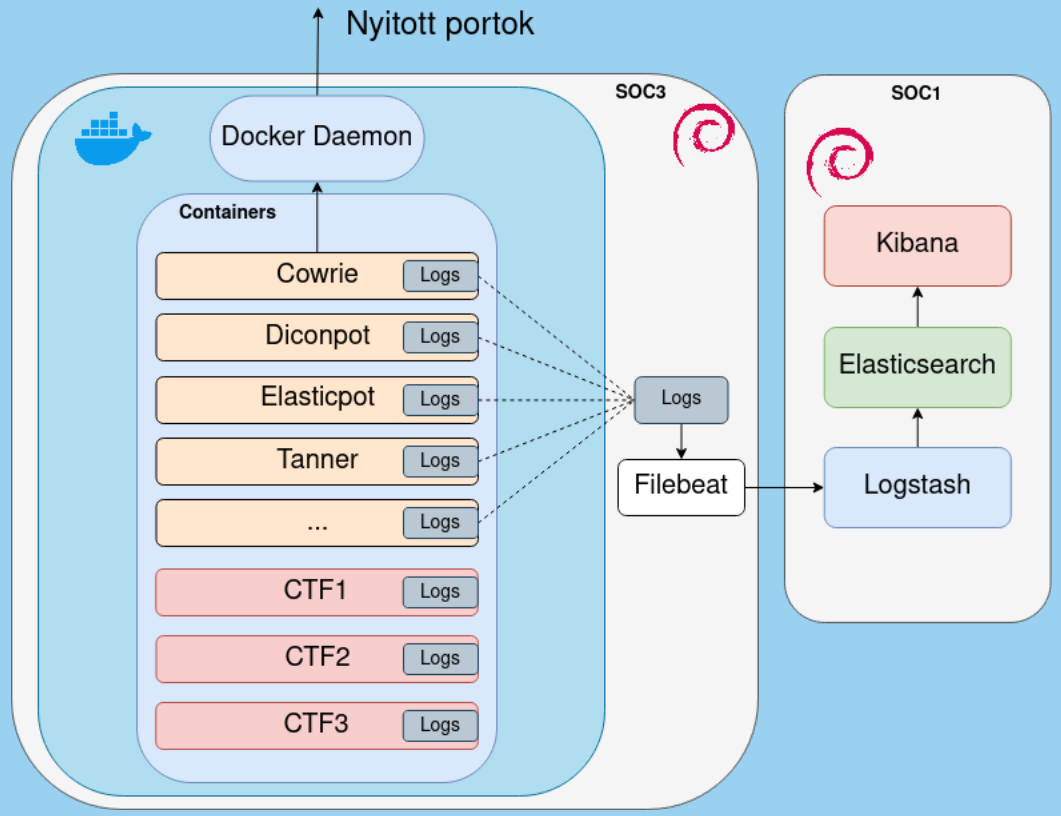
- Dr. Erdődi László
- Dr. Kail Eszter
- Rigó Ernő

- Érsok Máté
- Balogh Ádám (MSc)
- Scholtz Emanuel
- Hegedű Dániel

NIK-SOC
HONEYPOT
CTF
ATTACK GRAPH
V-SOC
5G SOC
CYBER RANGE

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Capture the flag - Zászlófoglalás



NIK-SOC
HONEYPOT
CTF
ATTACK GRAPH
V-SOC
5G SOC
CYBER RANGE

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Kérdések:

Milyen egy jó ctf platform?

Hogyan készítsünk dinamikuasn változó kihívásokat?

Hogyan mérjük a versenyzők szintjét?

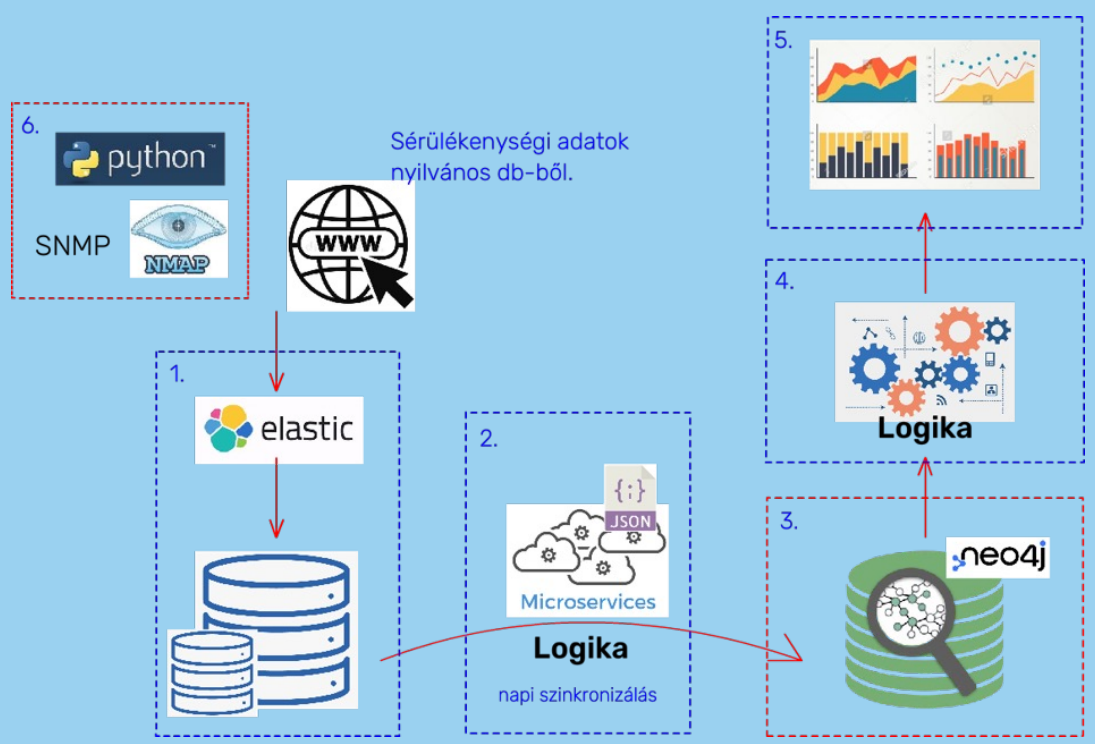
Hogyan rendezzünk versenyeket?

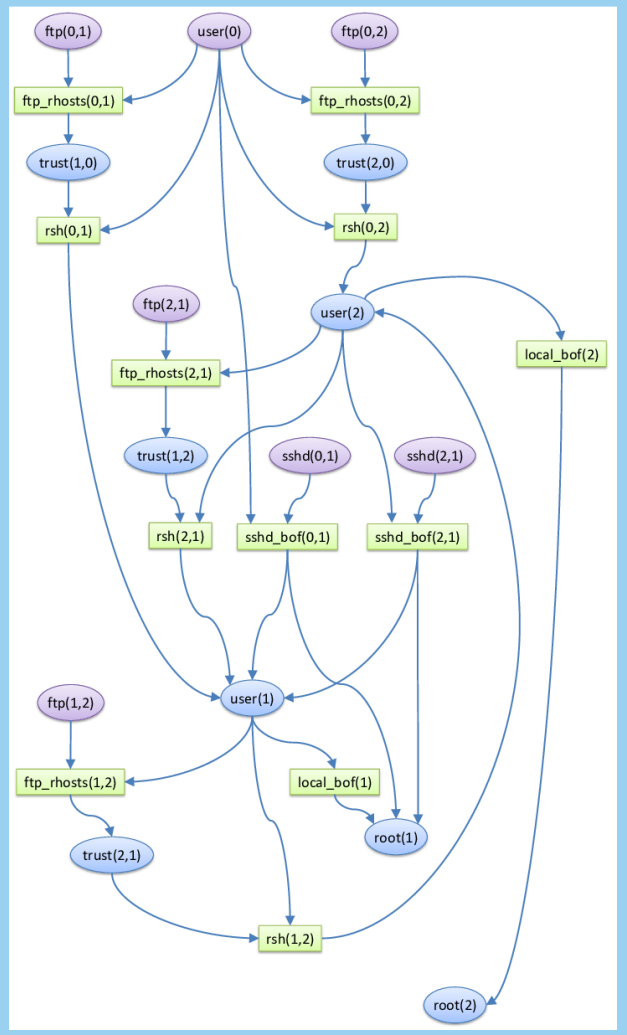
Tagok:

- Dr. Erdődi László

- Érsok Máté
- Balogh Ádám (MSc)
- Hegedűs Dani (BSc)
- Szabó Szabolcs
- Horváth Imre
- Vass Ádám
- Kotcauer Péter
- Barkó Zoltán
- Maronga Zsolt
- Léhner Donát

NIK-SOC
HONEYPOT
CTF
ATTACK GRAPH
V-SOC
5G SOC
CYBER RANGE





NIK-SOC
HONEYPOT
CTF
ATTACK GRAPH
V-SOC
5G SOC
CYBER RANGE

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Kérdések:

Milyen használati esetek definiálhatók?

Milyen adatokkal egészítsük ki a modellt támadások detektálásához?

Hogyan képes támogatni a logelemzést?

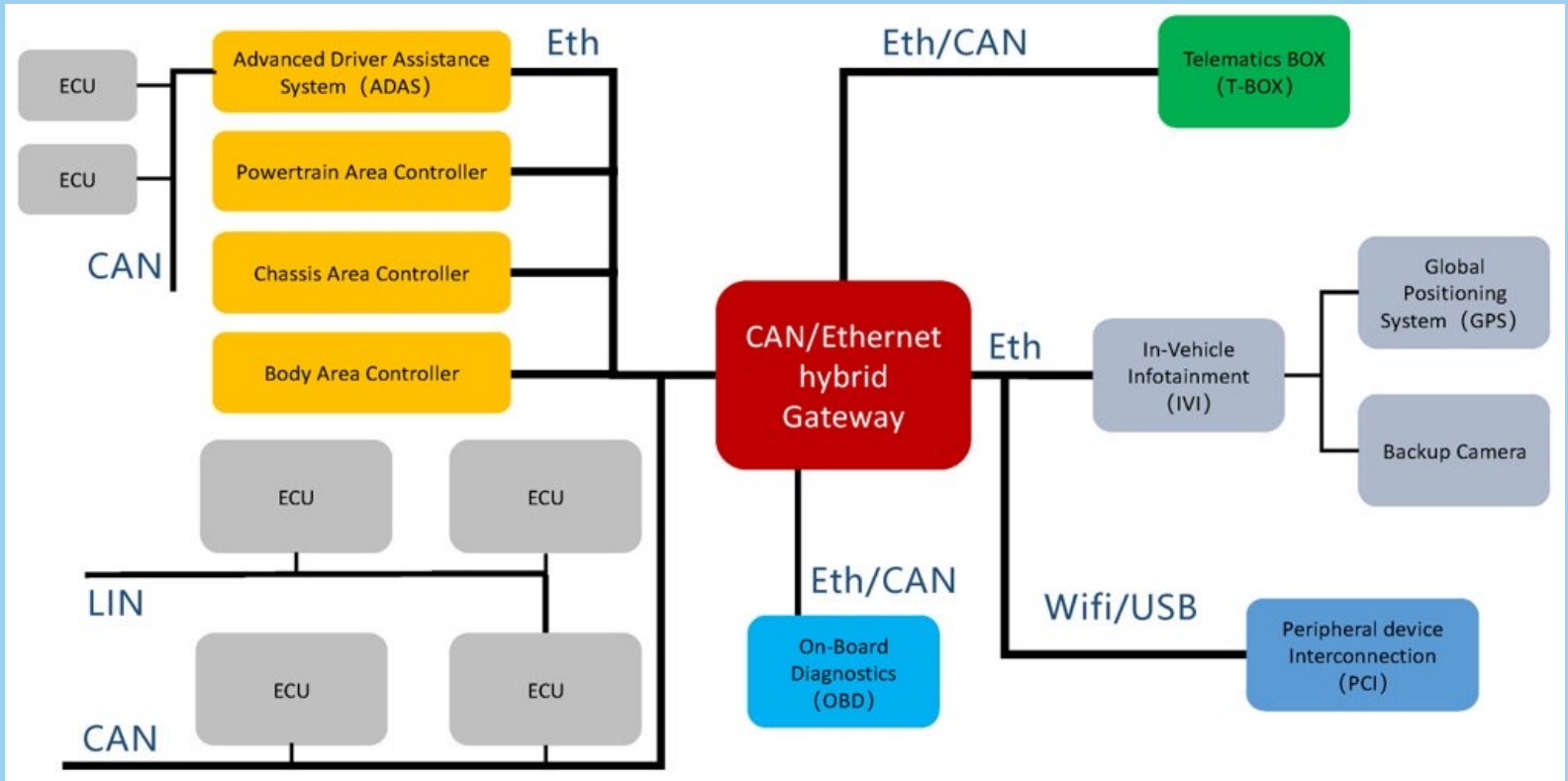
Hogyan támogassuk a SOC komponensek optimalizálását ?

Tagok:

- Dr. Fleiner Rita
- Márton Márk
- Dargó Krisztián

- Szöllősi Bence (BSc)
- Farkas Olivér (BSc)
- Újfalusi Zoltán (BSc)
- Sámson Norbert

NIK-SOC
HONEYPOT
CTF
ATTACK GRAPH
V-SOC
5G SOC
CYBER RANGE



NIK-SOC
HONEYPOT
CTF
ATTACK GRAPH
V-SOC
5G SOC
CYBER RANGE

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Kérdések:

Hogyan alakítsunk ki szimulációs környezetet?

Hogyan monitorozzuk a forgalmat?

Hogyan és miről gyűjtsünk logokat?

Hol gyűjtsük a logokat, az autóban vagy esetleg a felhőben?

Tagok:

- Dr. Csilling Ákos
- Dr. Kail Eszter
- Mera Abbassi (PhD)

- Iványi Bálint
- Burián Sándor
- Pozsonyi Tamás
- Nagy Róbert
- Can Katmis Ali
- Shugaa Addin Raidan

NIK-SOC

HONEYPOT

CTF

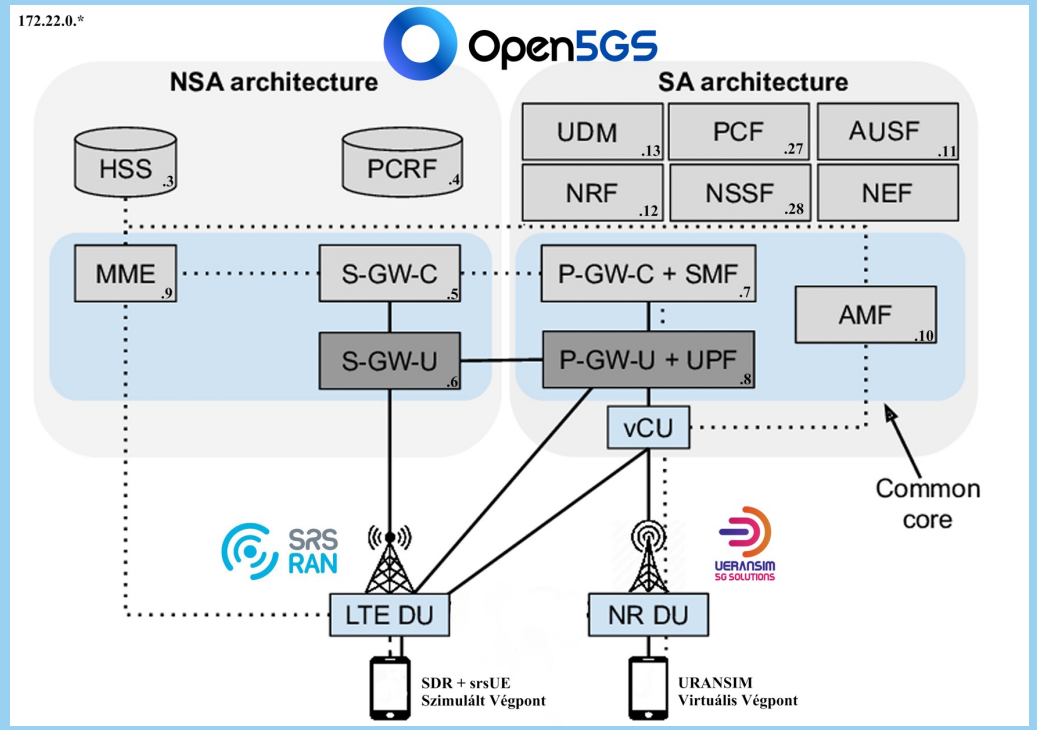
ATTACK GRAPH

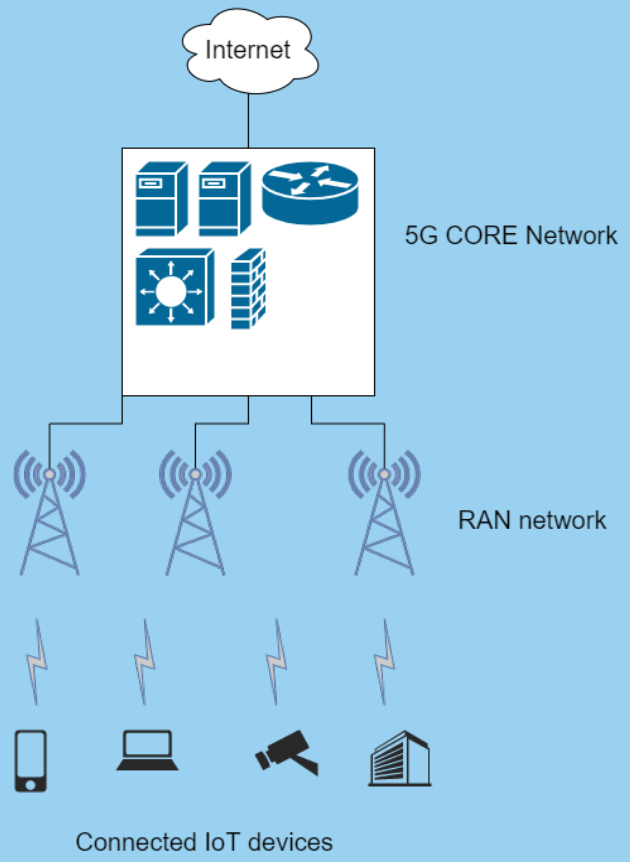
V-SOC

5G SOC

CYBER RANGE

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY





NIK-SOC
HONEYPOT
CTF
ATTACK GRAPH
V-SOC
5G SOC
CYBER RANGE

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Kérdések:

Hogyan gyűjtsünk naplóadatokat a végpontokról?

Milyen használati esetek kellenek egy SIEM-be?

Milyen támadásokat tudunk szimulálni?

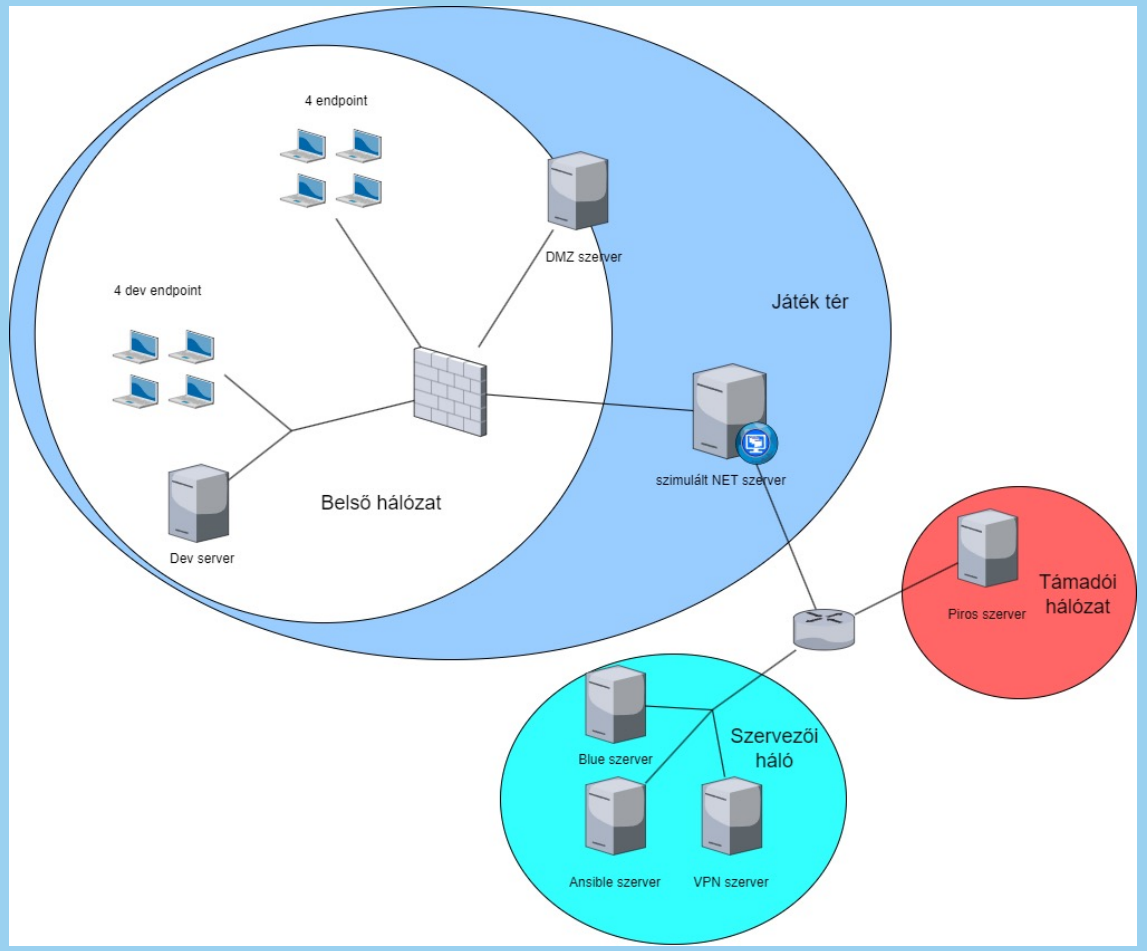
Tagok:

- Dr. Kail Eszter

- Bakos Dávid (BSc)
- Orsós Miklós (BSc)
- Kocsis Fruzsi (BSc)
- Török Roland (Kiber)
- Faragó Csaba (Kiber)
- Antalfia Benjamin (BSc)

NIK-SOC
HONEYPOT
CTF
ATTACK GRAPH
V-SOC
5G SOC
CYBER RANGE

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY



NIK-SOC
HONEYPOT
CTF
ATTACK GRAPH
V-SOC
5G SOC
CYBER RANGE

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Kérdések:

Milyen infrastruktúrát dolgozzunk ki és milyen eszközökkel?

Milyen támadási forgatókönyveket valósítsunk meg és hogyan ellenőrizzük az elhárítást?

Hogyan nyerjünk kibergyakorlatot Blue Team-ként?

Tagok:

- Kraudy Richárd (BSc)
- Verasztó Balász (BSc)
- Kövesdi Gábor (BSc)
- Juhász Péter (Kiber)
- Turai Tibor (Kiber)
- Kövesi Kristóf (Kiber)

NIK-SOC
HONEYPOT
CTF
ATTACK GRAPH
V-SOC
5G SOC
CYBER RANGE

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

banati.anna@nik.uni-obuda.hu

https://soc.uni-obuda.hu

https://honeylab.hu

5G kiberbiztonsági workshop

2022. november 16. | 14:00-17:00 | Óbudai Egyetem, NIK, F.06

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Köszönöm a figyelmet!

Click to edit Master title style