A HUN-REN SZTAKI HÁLÓZATBIZTONSÁG ÉS INTERNET TECHNOLÓGIÁK OSZTÁLY

NYÁRI SZAKMAI GYAKORNOKI PROGRAM

Kezdés: 2025. június 1-tól rugalmasan, a jelölttel egyeztetve

Időtartam: 6-8 hét

Munkavégzés helye: HUN-REN SZTAKI HBIT Részlege, 1111 Bp. Lágymányosi utca

Jelentkezés határideje: 2025. június 9.

A HUN-REN SZTAKI-ról röviden:

A HUN-REN Számítástechnikai és Automatizálási Kutatóintézet (HUN-REN SZTAKI) az ország legnagyobb és legsikeresebb informatikai kutatóintézete. A SZTAKI az informatika, az információtechnológia, számítástudomány és rokonterületei tudományának szakmai műhelye.

A HUN-REN SZTAKI gyakornoki programja:

A HUN-REN SZTAKI kiemelt hangsúlyt fektet a jövő kutatóinak, fejlesztő mérnökeinek kinevelésére, változatos projektmunkákat, mentorokat, eszközöket kínálunk megegyezés szerinti rugalmas munkarendben. Elkötelezettek vagyunk az iránt, hogy a leendő szakemberek minél magasabb minőségű és a piaci igényekhez jobban igazodó képzést kapjanak. Több hazai egyetemmel állunk szoros kapcsolatban, hogy ismereteinket, kutatás-fejlesztési tapasztalatainkat átadjuk a hallgatóinknak. A Gyakornoki Program során a hallgatók fejleszthetik a felhívásban szereplő téma elsajátítását és a gyakorlatban való megismerését.

A fogadó részleg rövid bemutatása:

Az osztály szakterületei közé tartoznak a hálózatbiztonsági felügyelő rendszerek fejlesztése, az azonosítási és jogosítási infrastruktúrák kiépítése, valamint a felhőalapú rendszerek. A Hun-CERT incidenskezelő központ üzemeltetése során, a hazai internetbiztonság területén szerzett tapasztalataikra támaszkodva, fejlesztik az ISZT tagjai számára incidenskezelési módszertanokat, valamint elősegítik a nemzetközi kapcsolattartást. További kiemelkedő eredmények közé tartozik a Probe projekt, mely egy valós idejű hálózatbiztonsági csapdarendszer. A részleg emellett aktívan részt vesz különböző nemzetközi projektekben, továbbá innovatív megoldásokat nyújt felhőalapú azonosítási technológiák fejlesztésére.

részleg linkje:

https://sztaki.hun-ren.hu/szervezet/reszlegek/hbit

A szakmai gyakorlat témája: **(HBIT-1) Nagy nyelvi modellek futtatása és kiértékelése lokális környezetben**

Feladatok:

A hallgató feladatai

1. Nagy nyelvi modellek futtatására alkalmas lokális környezet kialakítása. (Az ehhez szükséges hardvert biztosítjuk). A környezetnek alkalmasnak kell lennie különböző modellek futtatására, egyedi agentek kialakítására. Az általános emberi párbeszédre optimalizált modellek mellett fel kell kutatni olyan változatokat is, amelyek rendelkeznek kiberbiztonsági ismerettel.
2. A kiválasztott modellek teljesítménynek kiértékelése kiberbiztonsági témában. A kiértékelés meghatározott benchmark szerint történjen. Kitűzött cél. Hogy a modell részt tudjon venni az incidenskezelés ún. "triage" szakaszában, azaz biztonsági incidensek megerősítését, súlyosságának meghatározását segítő kérdésekre kell tudni értelmes válaszokat adnia.
3. A modellek használata során futó folyamatok, CPU terhelés, ezáltal az áramfogyasztás megfigyelése (a fogyasztás mérésére alkalmas eszközt és/vagy mérési eredményt biztosítunk). Továbbá a használat és az áramfogyasztás összefüggésére vonatkozó módszertan felkutatása és alkalmazása a kiértékelés/használat során

A feladat része az említett témák lehetőségeinek felkutatása, a meglévő eredmények figyelembevétele, a folyamat implementációja és dokumentálása, amely tartalmazza a feladat során szerzett tapasztalatokat, a felmerült problémákat és azok megoldásait, valamint javaslatokat a jövőbeni továbbfejlesztéshez.

Az előrehaladás a fenti prioritás mentén zajlik a rendelkezésre álló idő és erőforrások függvényében, a témavezető és a hallgató közös megegyezése alapján.

Elvárt tudás / készségek:

Docker ill. Linux operációs rendszerek telepítésére és használatára vonatkozó ismeretek, információbiztonsági alapismeretek

Munkavégzés helye: Budapest, XI.kerület , Kende utca/ Lágymányosi utca és/vagy online.

Jelentkezés módja: Önéletrajzzal elektronikus úton: **Komáromi Zoltán** gyakorlati témavezető részére a komzol@sztaki.hu, valamint „CC"-ben a hr@sztaki.hu e-mail címen.

A szakmai gyakorlat témája: **(HBIT-2) 5G felhasználási lehetőségei, korlátai és kockázatai ipari automatizálásban**

Feladat:

A feladat egy átfogó elemzés elkészítése az 5G mobiltechnológia ipari automatizálási környezetben történő alkalmazásának lehetőségeiről, technikai korlátairól, valamint az implementációval járó potenciális kockázatokról.

A hallgató feladatai:

- Szakirodalom és iparági esettanulmányok kutatása az 5G ipari alkalmazásairól (pl. okosgyárak, logisztika, robotika).
- Az 5G technológia azon kulcsfontosságú jellemzőinek (pl. alacsony késleltetés, nagy sávszélesség, hálózatszeletelés, megbízhatóság) azonosítása és elemzése, amelyek relevánsak az ipari automatizálás szempontjából.
- Potenciális felhasználási esetek tanulmányozása (pl. valós idejű folyamat-irányítás, prediktív karbantartás, távoli gépműködtetés, autonóm rendszerek stb).
- Választott felhasználási lehetőség implementálása és minősítése Campus 5G és Siemens 1200-as PLC segítségével

A beadott dokumentumnak tartalmaznia kell:

- Leírás a konkrét felhasználási eseteknek, kiemelve az 5G által nyújtott előnyöket (hatékonyságnövelés, új képességek stb.).
- Technikai, gazdasági és infrastrukturális kihívások elemzése, amelyek akadályozhatják a széleskörű elterjedést.
- A választott felhasználáshoz kapcsolódó protokoll implementációja egy alkalmas programozási nyelven, a mérés elvégzése és kiértékelése.

Elvárt tudás / készségek:

Hálózati és információbiztonsági alapismeretek, Docker, illetve programozási ismeretek

Munkavégzés helye: Budapest, XI.kerület , Kende utca/ Lágymányosi utca és/vagy online.

Jelentkezés módja: Önéletrajzzal elektronikus úton: **Radványi Patrik** gyakorlati témavezető részére a radvanyi.patrik.tamas@sztaki.hu, valamint „CC”-ben a hr@sztaki.hu e-mail címen.

Téma: **(HBIT-3) Ipari alacsony (field level) szintű protokollokon keresztül érkező fenyegetések és azok beemelése a kockázatelemzésbe**

Feladat:

A feladat célja az ipari vezérlőrendszerek (ICS/OT) legalacsonyabb, ún. terepi (field) szintjén használt kommunikációs protokollokon (pl. Modbus, Profibus, CAN, EtherCAT) keresztül érkező specifikus kiberfenyegetések elemzése. További cél egy gyakorlati módszertan vagy ajánlásrendszer kidolgozása arra vonatkozóan, hogyan lehet ezeket a gyakran figyelmen kívül hagyott, de kritikus veszélyforrásokat hatékonyan beemelni a vállalatok standard IT/OT kiberbiztonsági kockázatelemzési folyamataiba.

Főbb feladatok:

- Kutatás a legelterjedtebb ipari terepi szintű protokollok működéséről, felépítéséről és azok inherens biztonsági gyengeségeiről (pl. hitelesítés, titkosítás hiánya).
- E protokollokat célzó ismert és potenciális támadási vektorok, fenyegetéstípusok (pl. adatmanipuláció, parancsinjektálás, üzenet-visszajátszás, szolgáltatásmegtagadás) azonosítása és kategorizálása.
- Ipari környezetben alkalmazott kockázatelemzési módszertanok (pl. NIST SP 800-30, IEC 62443 kockázatértékelési részei) áttekintése abból a szempontból, hogyan kezelik (vagy nem kezelik) a terepi szintű protokollok kockázatait.
- Választott protokollon legalább két támadási vektor bemutatása.

A beadott munkának tartalmaznia kell:

- Kulcsfontosságú protokollok (pl. Modbus RTU/TCP, Profibus DP/PA, CANopen, EtherNet/IP, EtherCAT) rövid ismertetése és jellemző biztonsági hiányosságaik elemzése.
- Leírás a protokoll-specifikus fenyegetéseknek, támadási forgatókönyveknek és azok lehetséges hatásainak az ipari folyamatokra és a biztonságra.
- Javasolt keretrendszer vagy lépéssorozat bemutatása, amely lehetővé teszi a terepi szintű fenyegetések azonosítását, értékelését (valószínűség, hatás) és beillesztését a meglévő kockázatkezelési folyamatokba. Kitérhet a releváns kontrollok azonosítására is.
- A választott protokoll implementációja egy alkalmas programozási nyelven, valamint két mérési jegyzőkönyv a támadásról Siemens 1200-as PLC ellen.

Elvárt tudás / készségek:

Hálózati és információbiztonsági alapismeretek, ipari protokollok ismerete előny, Docker, illetve programozási ismeretek

Munkavégzés helye: Budapest, XI.kerület , Kende utca/ Lágymányosi utca és/vagy online.

Jelentkezés módja: Önéletrajzzal elektronikus úton: **Radványi Patrik** gyakorlati témavezető részére a radvanyi.patrik.tamas@sztaki.hu, valamint „CC”-ben a hr@sztaki.hu e-mail címen.

Téma: **(HBIT-4) Evil PLC típusú támadások ismert formái és beemelésének lehetőségei a kockázatelemzésbe**

Feladat:

A feladat célja az ipari irányítórendszerek (ICS/OT) központi elemeit, a programozható logikai vezérlőket (PLC) érintő, ún. "Evil PLC" támadások ismert formáinak és megvalósítási technikáinak részletes feltárása. Ezek olyan támadások, ahol a PLC-t kompromittálják, rosszindulatú logikával látják el, vagy egyenesen egy kártékony, de legitimnek tűnő eszközt juttatnak a rendszerbe. A feladat további célja, hogy gyakorlati javaslatokat fogalmazzon meg arra vonatkozóan, hogyan lehet ezen specifikus és nagy kockázatú fenyegetéseket hatékonyan beépíteni a vállalati kiberbiztonsági kockázatelemzési folyamatokba.

Főbb feladatok

- Az "Evil PLC" koncepcióval kapcsolatos szakirodalom, publikált kutatások, és esettanulmányok (pl. biztonsági konferenciákon bemutatott proof-of-concept támadások) felkutatása és elemzése.
- Az ismert "Evil PLC" támadási módszerek kategorizálása (pl. mérnöki munkaállomás (EWS) kompromittálása, PLC firmware sebezhetőségeinek kihasználása, manipulált logika feltöltése hálózaton vagy fizikailag, ellátási láncon keresztüli támadás).
- A létező és lehetséges detektálási és megelőzési technikák vizsgálata (pl. PLC programkód-integritás ellenőrzése, futásidejű viselkedésanalízis, hálózati szegmentáció, EWS biztonságának erősítése).
- Támadás detektálására alkalmas gateway funkció implementációja Siemens TIA Portal és S7-1200-es PLC között

A beadott dokumentumnak tartalmaznia kell:

- A különböző támadási technikák bemutatása, működési elvük és megvalósításuk módja (technikai részletekkel).
- Annak elemzése, hogy a támadók milyen utakon (pl. hálózat, fizikai hozzáférés, social engineering) érhetik el céljaikat, és milyen tipikus támadási láncok képzelhetők el.
- Implementáció választott programozási nyelven, mérési jegyzőkönyvek a támadás szimulációjáról és detektálásáról

Elvárt tudás / készségek:

Hálózati és információbiztonsági alapismeretek, ipari protokollok és eszközök ismerete előny

Munkavégzés helye: Budapest, XI.kerület , Kende utca/ Lágymányosi utca és/vagy online.

Jelentkezés módja: Önéletrajzzal elektronikus úton: **Radványi Patrik** gyakorlati témavezető részére a radvanyi.patrik.tamas@sztaki.hu, valamint „CC”-ben a hr@sztaki.hu e-mail címen.

Téma: **(HBIT-4.1) Felhőbeli erőforrásokra támaszkodó OT rendszerek fenyegetései**

Feladat:

A feladat egy elemzés készítése azokról a kiberbiztonsági fenyegetésekről, amelyek az OT (Operational Technology) rendszerek és a felhőalapú platformok integrációjából fakadnak. További feladat egy kiválasztott, releváns fenyegetési forgatókönyv gyakorlati demonstrálása tesztkörnyezetben és bemutatva lehetséges védekezési mechanizmusokat.

Főbb feladatok

- Jellemző OT-felhő integrációs architektúrák és felhasználási esetek elemzése. Specifikus fenyegetési vektorok, sebezhetőségek és potenciális támadási forgatókönyvek azonosítása az OT-felhő kontextusában.
- Egy laboratóriumi tesztkörnyezet megtervezése és kialakítása OpenStack virtuális gépek és egy S7-1200 PLC felhasználásával, egy OT-felhő integrációs forgatókönyv modellezésére.
- Az eredményeinek összefoglalása.

A beadott dokumentumnak tartalmaznia kell:

- OT rendszerek és felhőintegráció áttekintése.
- A tesztkörnyezet felépítése és a demonstrált fenyegetési forgatókönyv részletes leírása, a támadás lépései és eszközei.
- A támadás hatásainak bemutatása és a megfigyelt eredmények kiértékelése.

Elvárt tudás / készségek:

Hálózati és információbiztonsági alapismeretek, ipari protokollok és eszközök ismerete előny, felhőtechnológiák ismerete

Munkavégzés helye: Budapest, XI.kerület , Kende utca/ Lágymányosi utca és/vagy online.

Jelentkezés módja: Önéletrajzzal elektronikus úton: **Radványi Patrik** gyakorlati témavezető részére a radvanyi.patrik.tamas@sztaki.hu, valamint „CC”-ben a hr@sztaki.hu e-mail címen.

A szakmai gyakorlat témája: **(HBIT-5) IPv6 bevezetés tervezése**

Feladatok:

A hallgató feladata, hogy feltérképezze a SZTAKI-ban jelenleg működő IPv4 hálózatot, majd ennek alapján tervezze meg az IPv6 hálózatot figyelembe véve az egy-két VLAN-ban már megvalósított IPv6 szigeteket is.

A megtervezett rendszernek tartalmaznia kell:

- A jelenlegi hálózati topológiát
- A kiosztandó címtartományokat VLAN-ok szerint
- Az implementáció ütemezését, lépéseit
- Az egyes lépések után szükséges tesztelési eseteket

Elvárt tudás / készségek:

Erős hálózati ismeretek, javasolt Cisco és/vagy Huawei hálózati eszközök ismerete is

Munkavégzés helye: Budapest, XI.kerület , Kende utca/ Lágymányosi utca és/vagy online.

Jelentkezés módja: Önéletrajzzal elektronikus úton: **Ormos Pál** gyakorlati témavezető részére a ormos@sztaki.hu, valamint „CC”-ben a hr@sztaki.hu e-mail címen.

A szakmai gyakorlat témája: **(HBIT-6) Cyber Threat Intelligence adatforrások integrációja és elemzése**

Feladatok:

A hallgató feladatai

Az IntelMQ és MISP adatforrások integrációja, valamint külső IT asset inventory (IP cím és domain név listák, szoftver listák) készletek fejlesztése. A rendszernek képesnek kell lennie a fent említett források összehangolt használatára, hogy megbízható és következetes fenyegetettségi információkat generáljon.

Külső IT asset inventory alapján a fenyegetettségi információk priorizálása. A MISP-ből kigyűjtött CTI (Cyber Threat Intelligence) események alapján riasztási helyzetek azonosítása. A feladat célja a releváns veszélyforrások előrejelzése a rendelkezésre álló adatokra támaszkodva.

Az integrált rendszer által generált riasztási helyzetek vizsgálata és optimalizálása. Ennek során a duplikált és fals pozitív riasztások kiszűrése kiemelt jelentőségű, a rendszer hatékonyságának maximalizálása érdekében.

A témakörhöz kapcsolódó irodalomkutatási és dokumentációs feladatok elvégzése, beleértve a témához kapcsolódó legújabb kutatási eredmények és módszertani elvek feltérképezését.

A feladat része a témák lehetőségeinek feltárása, a meglévő eredmények figyelembevétele, valamint az implementációs és dokumentációs munka, amely tartalmazza a projekt során szerzett tapasztalatokat, a felmerült problémák elemzését és megoldását, továbbá javaslatokat a jövőbeni fejlesztésekhez.

Az előrehaladás a rendelkezésre álló idő és erőforrások függvényében zajlik a témavezető és a hallgató közös megegyezése alapján.

Elvárt tudás / készségek:

Docker és Linux operációs rendszerek telepítésére és használatára vonatkozó ismeretek. Információbiztonsági alapismeretek. Alapvető programozási és adatkezelési ismeretek, különösen Python nyelvben.

Munkavégzés helye: Budapest, XI. kerület, Kende utca/ Lágymányosi utca és/vagy online.

Jelentkezés módja: Önéletrajzzal elektronikus úton. **Rigó Ernő** gyakorlati témavezető részére a rigo@sztaki.hu, valamint „CC”-ben a hr@sztaki.hu e-mail címen

A szakmai gyakorlat témája: **(HBIT-7) Generatív MI benchmarkok vs. környezeti lábnyom**
Feladatok:

Erre a feladatkiírásra informatikusokon kívül energetikai mérnökök, környezetmérnökök, a téma iránt érdeklődő gépész- mechatronikai és villamosmérnökök jelentkezését is várjuk. Előnyt élveznek a publikációs lehetőségek, pl. TDK iránt érdeklődők és akik PhD képzésre készülnek.

A hallgató feladatai

1. Generatív MI: nagy nyelvi modellek, kép- hang- videogenerálók, programkód-generátorok értékelésére használt benchmarkok felkutatása, azok képességeinek elemzése, különösen abból a szempontból, hogy környezeti lábnyom becslésére mennyire alkalmasak. Potenciálisan együttműködés más gyakornok(ok)kal akik feladata LLM-ek lokális telepítése lesz ugyanebben az időszakban, de a szolgáltatásként igénybe vehető MI-k is fókuszban vannak.
2. A kiválasztott benchmarkok kiértékelése, összehasonlítása megadott szempontrendszer szerint környezeti lábnyom mérése szempontjából. A szempontrendszer kialakításáért egy kutatócsapat felelős, amelynek a hallgató része lesz.
3. Az előző pont kimenetétől függően benchmarkok továbbfejlesztése, kritikája, bővítése.
4. Részvétel publikációk készítésében, amelyhez képzést biztosítunk.

Elvárt tudás / készségek:

Kritikus gondolkodás, felhasználói tapasztalat generatív MI-vel, angol nyelv: erős olvasás, legalább közepes írás, tanulásra való képesség. Előnyt jelentenek a fenntarthatósággal kapcsolatos ismeretek.

Munkavégzés helye: Budapest, XI.kerület , Kende utca/ Lágymányosi utca és/vagy online.

Jelentkezés módja: Önéletrajzzal elektronikus úton: **Héder Mihály** gyakorlati témavezető részére a heder.mihaly@sztaki.hu, valamint „CC”-ben a hr@sztaki.hu e-mail címen.