A HUN-REN SZTAKI HÁLÓZATBIZTONSÁG ÉS INTERNET TECHNOLÓGIÁK OSZTÁLY
NYÁRI SZAKMAI GYAKORNOKI PROGRAM

Kezdés: 2024. június 1-től rugalmasan, a jelölttel egyeztetve

Időtartam: 6-8 hét

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

Jelentkezés határideje: 2024. június 3.

Jelentkezés módja: rigo@sztaki.hun-ren.hu e-mail címre küldött jelentkezés illetve cc: hr@sztaki.hun-ren.hu

(CV, motivációs levél, téma preferenciák megjelölése szükséges)

A HUN-REN SZTAKI-ról röviden:

A HUN-REN Számítástechnikai és Automatizálási Kutatóintézet (HUN-REN SZTAKI) az ország legnagyobb és legsikeresebb informatikai kutatóintézete. A HUN-REN 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:

Csatlakozz a Hálózatbiztonság és Internet Technológiák osztály csapatához, vegyél részt izgalmas projektekben, amelyek a legújabb technológiákat alkalmazzák a biztonságos és megbízható online környezet megteremtéséhez!

Mit kínálunk:

- Változatos munkakörnyezet és feladatok: biztonsági tervezés, tesztelés és ellenőrzés, azonosítási megoldások, biztonsági vizsgálatok, incidenskezelés, fejlesztés és tesztelés, rendszerintegráció
- Robusztus nyílt technológiák: IaaS/PaaS cloud infrastruktúra programozás (Infrastructure as Code), konténer orkesztráció (Kubernetes), Linux/Unix környezet, változatos programnyelvek (Java, Python, PHP, Shell, Typescript)
- Tudományos kutatás: lehetőség a biztonsági megoldások és szoftver-keretrendszerek kutatásában, tervezésében való részvételre egyetemi szinten
- Fejlődési lehetőségek: folyamatos tanulás és fejlődés a legújabb technológiák elsajátításával, rugalmas kísérleti és kutatási projektek keretében
- Barátságos munkakörnyezet, távoli munkavégzés lehetősége, nagy szaktudású kollégák.

Ha:

- Érdekelnek a nyílt internetes technológiák
- Fontos számodra a kiberbiztonság
- Szeretnél tanulni és fejlődni

Akkor itt a helyed!

részleg linkje:

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

HUN REN | SZTAKI

Téma: Korszerű authentikációs infrastruktúra kialakítása IaC módszerrel

Feladat:

A RADIUS alapú authentikáció, autorizáció, valamint az erre épülő accounting (AAA) elengedhetetlen az intézeti WiFi, VPN szolgáltatás működése és a hálózati eszközök azonosítási folyamatai során.

A gyakornok feladata egy jelenleg is üzemelő szolgáltatási környezet mintája alapján új, tartalékolt RADIUS szolgáltatás megtervezése, majd implementációja. A megvalósított környezetben a FreeRADIUS3 legfrissebb verziójának használata elvárt. A bevezetendő redundáns RADIUS szolgáltatás az intézet által üzemeltetett központi LDAP névtár, mint elsődleges adatforrás mellett együttműködik a nemzetközi EduROAM RADIUS föderációval is, lehetővé téve a távoli együttműködő partnerintézmények felhasználóinak azonosítását is. Az új szolgáltatás kialakítása az accounting információk gyűjtését és webes megjelenítését is magában foglalja, ennek keretében szükséges az üzem során keletkező adatok központi logszerverre történő továbbítása és elemzése is. A kialakításra kerülő szolgáltatást legalább alapszinten integrálni kell a prometheus/grafana alapú felügyeleti rendszerbe. A naplóelemző és felügyeleti rendszerekben RADIUS dashboardok kialakítása opcionális feladat.

Az új rendszert Infrastructure as Code (IaC) mintamegoldás formájában kell kidolgozni, legalább konténerizált (Docker), de célszerűen Kubernetes környezetben, oly módon, hogy a megoldás a HUN-REN kutatóhálózat bármely intézményében is használható legyen.

A feladat elvégzéséhez biztosított eszközök és komponensek:

Linux alapú virtualizációs és konténerizációs környezet és/vagy k8s cluster, LDAP alapú címtár szolgáltatás, OpenSearch alapú központi naplógyűjtő- és elemző rendszer, Prometheus / Grafana alapú központi felügyeleti rendszer, GitLab projektkezelő és szoftver repozitórium.

A jelentkezőtől elvárt előzetes ismeretek:

Linux alapú környezet alapszintű adminisztrációs ismerete. Konténerizációs technológiák és git verziókezelő alapszintű ismerete. A RADIUS, LDAP, OpenSearch, Prometheus technológiák előzetes ismerete nem elvárt, ezek megismerése a feladat része.

Mentor: Ormos Pál

HUN REN | SZTAKI

Téma: Netflow/sflow/jflow adatgyűjtő rendszer kialakítása NoSQL alapon

Feladat:

A központi hálózati eszközökön megjelenő forgalom fő jellemzőit rögzítő netflow/sflow stb. adatok gyűjtése és elemzése elengedhetetlen ahhoz, hogy bármilyen hálózati üzemviteli vagy biztonsági esemény (incidens) esetén gyorsan, pontos adatokkal alátámasztva lehessen reagálni, esetlegesen egy az infrastruktúrát érintő támadást előre is jelezni lehessen.

A gyakornok feladata a jelenleg üzemelő Neflow / nfsen infrastruktúra mintája alapján új hálózati forgalomgyűjtő- és elemző megoldás megtervezése és implementációja. A megvalósítás során az adatokat a jelenlegi rendszer párhuzamos üzemének fenntartása mellett a hallgató rendelkezésére bocsátott központi OpenSearch szolgáltatás részére is továbbításra kerül, ahonnan azt fel kell dolgozni, meg kell jeleníteni. A korábbi rendszer hosszú távon rögzített adatait a megvalósítás során lehetőség szerint migrálni kell az új rendszerbe is, valamint biztosítani kell a hálózati forgalom keresési és riportolási lehetőségeket az új környezetben, ennek érdekében a jelenlegi riportolási rendszer mintája alapján OpenSearch dashboardok megtervezése és kialakítása a hallgató feladatának része. A kialakításra kerülő szolgáltatást legalább alapszinten integrálni kell a prometheus/grafana alapú felügyeleti rendszerbe.

Az új rendszert Infrastructure as Code (IaC) mintamegoldás formájában kell kidolgozni, legalább konténerizált (Docker), de célszerűen Kubernetes környezetben, oly módon, hogy a megoldás a HUN-REN kutatóhálózat bármely intézményében is használható legyen.

A feladat elvégzéséhez biztosított eszközök:

Linux alapú virtualizációs és konténerizációs környezet és/vagy k8s cluster, Netflow/Sflow adatforrások, OpenSearch alapú központi naplógyűjtő- és elemző rendszer, Prometheus / Grafana alapú központi felügyeleti rendszer, GitLab projektkezelő és szoftver repozitórium.

A jelentkezőtől elvárt előzetes ismeretek:

Linux alapú környezet alapszintű adminisztrációs ismerete. Konténerizációs technológiák és git verziókezelő alapszintű ismerete. A Netflow/Sflow, OpenSearch, Prometheus technológiák előzetes ismerete nem elvárt, ezek megismerése a feladat része.

Mentor: Ormos Pál

Téma: HunCERT Security Feed data pipeline kialakítása IntelMQ alapon

Feladat:

A mai digitális korban a kiberfenyegetések egyre kifinomultabbá és pusztítóbbá válnak. A vállalatoknak és a szervezeteknek elengedhetetlen a hatékony kiberbiztonsági stratégiák kidolgozása és fenntartása az adatok és rendszerek védelme érdekében. A Cyber Threat Intelligence (CTI) kulcsfontosságú szerepet játszik ebben a törekvésben. A CTI olyan információk gyűjtése, elemzése és terjesztése, amelyek a kiberfenyegetésekkel, sebezhetőségekkel és támadásokkal kapcsolatosak. Segít a szervezeteknek megérteni a fenyegető tájat, felismerni a potenciális kockázatokat, és proaktív lépéseket tenni a támadások megelőzése érdekében.

A gyakornok feladata a HUN-REN SZTAKI által nyújtott HunCERT (https://cert.hu) incidenskezelő szolgáltatás szakértői számára különböző formátumokban és csatornákon rendelkezésére álló, nyílt vagy korlátozott hozzáférésű hálózati biztonsági adatforrások integrációja az IntelMQ (https://intelmq.readthedocs.io/) alapú CTI platform segítségével. A hallgató feladata az IntelMQ megismerése és feltérképezése, a szolgáltatás megtervezése és kialakítása, kezdeti konfigurációja, valamint a rendelkezésére álló biztonsági adatforrások feltérképezése, egyéb szakrendszerekkel történő integrációja és tesztelése. További feladat a rendelkezésre álló adatok hasznosítási lehetőségeinek áttekintése és javaslatok megtétele a HunCERT incidenskezelési tevékenységének vonatkozásában.

Az új rendszert Infrastructure as Code (IaC) mintamegoldás formájában kell kidolgozni, legalább konténerizált (Docker), de célszerűen Kubernetes környezetben. A kialakításra kerülő szolgáltatást legalább alapszinten integrálni kell a prometheus/grafana alapú felügyeleti rendszerbe. A naplóelemző és felügyeleti rendszerekben RADIUS dashboardok kialakítása opcionális feladat.

A feladat elvégzéséhez biztosított eszközök és komponensek:

Linux alapú virtualizációs és konténerizációs környezet és/vagy k8s cluster, potenciális biztonsági adatforrások, OpenSearch alapú központi naplógyűjtő- és elemző rendszer, EasyRedmine eseménykezelő rendszer, Prometheus / Grafana alapú központi felügyeleti rendszer, GitLab projektkezelő és szoftver repozitórium.

A jelentkezőtől elvárt előzetes ismeretek:

Linux alapú környezet alapszintű adminisztrációs ismerete. Konténerizációs technológiák és git verziókezelő alapszintű ismerete. A CTI koncepciók és az IntelMQ, valamint az ezekhez kapcsolódó specializált technológiák előzetes ismerete nem elvárt, ezek megismerése a feladat része.

Mentor: Rigó Ernő

Téma: Támadási gráf építő eljárás továbbfejlesztése Neo4j környezetben

Feladat:

A támadási gráfok a kiberbiztonság értékelésének területén használt eszközök, amelyek vizuálisan ábrázolják egy számítógépes rendszer potenciális sebezhetőségeit és a támadások lehetséges útvonalait. A kockázatértékelés során a támadási gráfok kulcsfontosságúak a lehetséges fenyegetések azonosításában és értékelésében, valamint a hatékony védelmi stratégiák kidolgozásában.

A gyakornok feladata a HUN-REN SZTAKI által folytatott biztonságkutatási tevékenység keretében kifejlesztett támadási gráf konstrukciós eljárás kiegészítése oly módon, hogy a jelenlegi egy ciklusra épülő adatfeldolgozási folyamat folyamatossá váljon. A jelenlegi megvalósítás működése során támadási gráf előállításához felhasznált különböző adatforrások (hálózati forgalmi adatok, sérülékenységvizsgálati eredmények, külső biztonsági információk) feldolgozása kötegelten, szekvenciálisan zajlik. A hallgató feladata a jelenleg elérhető kötegelt megvalósítás áttekintése, újratervezése és kiegészítő implementációja oly módon, hogy az képes legyen az adatforrások inkrementális változásainak követésére, a létrehozott támadási gráf követő módosítására.

A feladat elvégzéséhez biztosított eszközök és komponensek:

Támadási gráf kutatási és fejlesztési környezet a jelenlegi adatfeldolgozási folyamat Python alapú implementációjával, valamint a feldolgozáshoz szükséges adatforrásokkal és Neo4j alapú gráfadatbázis környezettel.

A jelentkezőtől elvárt előzetes ismeretek:

Python programozási ismeretek. Gráf adatszerkezetek és gráfprogramozás alapszintű ismerete (NetworkX ismerete előny). A Neo4j cypher lekérdezési nyelv, a támadási gráfok és ezekre épülő algoritmusok előzetes ismerete nem elvárt, ezek megismerése a feladat része.

Mentor: Rigó Ernő

Téma: Forensics eszköz tervezése és fejlesztése kártékony e-mailekből történő adatrögzítéshez

Feladat:

A kártékony e-mailek, különösen a phishing levelek komoly biztonsági kockázatot jelentenek a személyes adatokra és a számítógépes rendszerekre nézve. Ezek a levelek arra törekszenek, hogy megtévesszék a címzettet, és rávegyék arra, hogy adja meg személyes adatait, például jelszavakat, bankkártya adatokat, vagy kattintson egy fertőzött linkre. A phishing levelek gyakran úgy tűnnek, mintha megbízható forrásból származnának, például bankoktól, webáruházaktól, vagy közösségi média platformoktól. A levélben szereplő szöveg és a külső megjelenés megtévesztően professzionális lehet, ami megnehezíti a hamis levelek azonosítását.

A Hallgató feladata a rendelkezésére bocsátott kártékony e-mail üzenetekben alkalmazott támadási módszerek átfogó vizsgálata alapján egy olyan automatizált eljárás kidolgozása, valamint az ezt támogató szoftver eszköz kifejlesztése, mely egy szakértő által előzetesen már kártékonynak minősített e-mail üzenetből bizonyítékrögzítés céllal strukturált metaadatokkal ellátott elemi tényadatok kiemelését és strukturált formában történő tárolását támogatja. A tényadatok körének pontosabb kidolgozása, meghatározása a hallgató feladata, de ezek célszerűen kiterjednek az üzenetből közvetlenül kinyerhető adatok (feladó, címzett, szöveges- és képelemek, képernyőkép, URL-ek) mellett a hivatkozott külső erőforrásokra (pl. adathalász weboldal címe, képernyőképe, akár többszörös átirányítások követésével), illetve egyéb külső forrásokból kinyerhető támogató információkra (pl. geolokáció, DNS, ASN, Whois, RBL adatok) is.

A bizonyítékrögzítés során előálló adatcsomagot a MISP által támogatott szabványos objektum sémák valamelyikére kell illeszteni (https://www.misp-project.org/objects.html). A MISP API használata az output adatok rögzítésére a feladat megvalósítás során nem kötelező, de javasolt.

A feladat elvégzéséhez biztosított eszközök és komponensek:

Kártékony e-mail üzenetek (tesztadatok) gyűjteménye, Linux alapú szoftverfejlesztési környezet.

A jelentkezőtől elvárt előzetes ismeretek:

Programozási ismeretek (javasolt: Python), alapszintű hálózati ismeretek, e-mail és web szolgáltatások protokolljainak, adatformátumainak alapszintű ismerete.

Mentor: Rigó Ernő