

Kibernetiniai nusikaltimai be sienų

Tarptautinis bendradarbiavimas, kuriant mokymų programas
teisėsaugos pareigūnų gebėjimams stiprinti



Kibernetinė erdvė

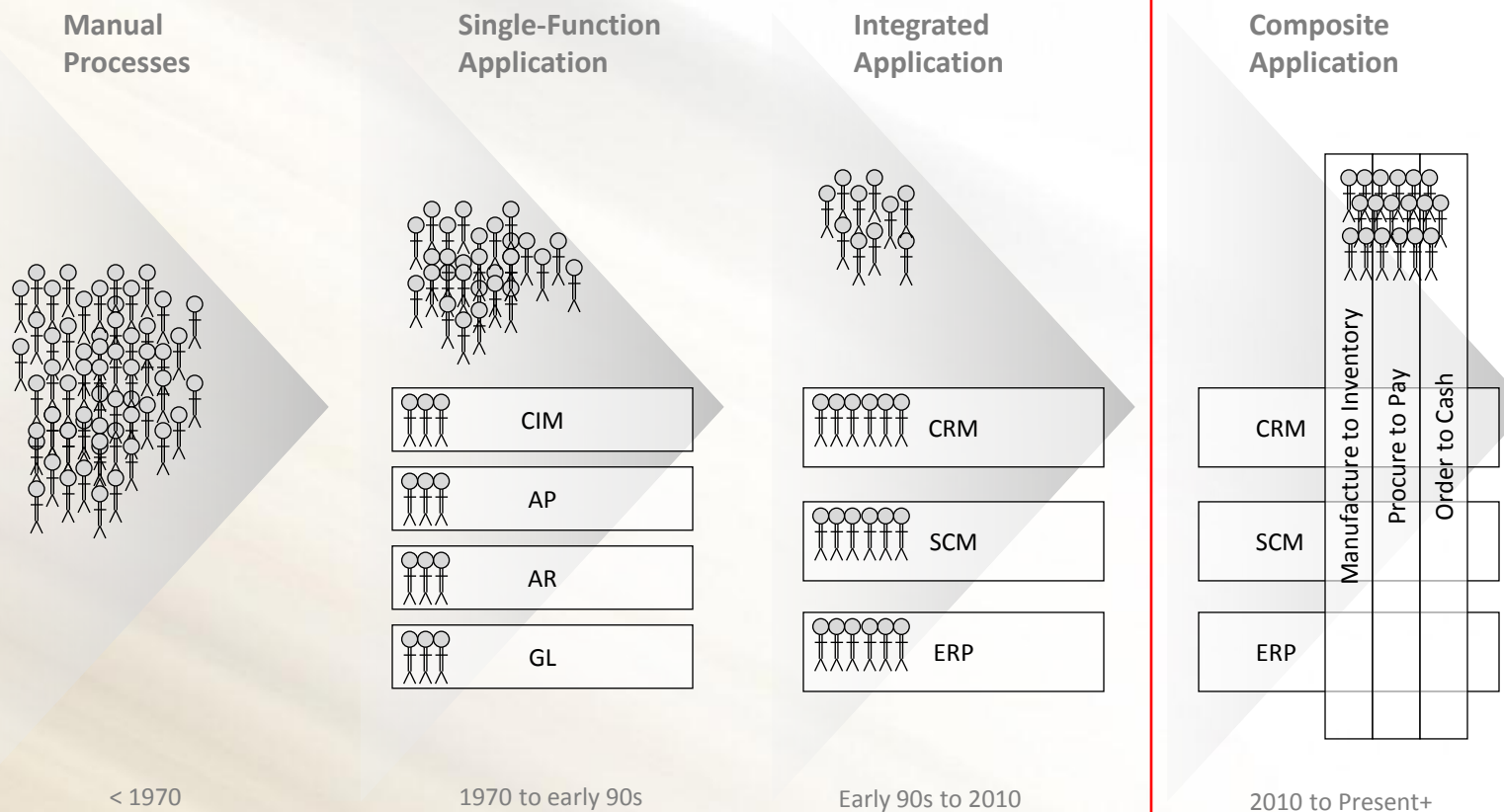
- Dinamiškiausia iš sričių
- Apimanti visas gyvenimo sritis
- Viena jauniausių iš mokslo tyrimo sričių
- Mažiausiai reglamentuota

Tendencijos ir greitis

- Kelių infrastruktūrai yra tiek pat metų kiek ir mūsų civilizacijai
- Komercinei draudimo veiklai – 800 metų
- Dvejybinio įrašo apskaitai – 500 metų
- Atominei energetikai – 60 metų
- Internetui – 25 metai
- Socialiniam internetui – 10 metų
- Technologijos naudojamumo ir sklaidos greitis (50 mln naudotojų):
 - Radijas -> 38 metai
 - Televizija -> 13 metų
 - Internetas -> 4 metai
 - iPod -> 3 metai
 - Facebook -> 2 metai

Sveikiname,
Jūs pajungti 😊

Kaip mes taip?



Piktoji progreso pusė...

Įsilaužimas į išmaniuosius įrenginius Reputacijos kompromitavimas
Informacijos slėpimas DDOS atakos Kontaktinės informacijos vagystė
Organizuotas nusiklastamumas – socialinė inžinerija Asmens tapatybės vagystė
Slaptos informacijos atskleidimas Šalies saugumo informacija
Prieš valstybę ar visuomenę nukreiptas radikalios nuomonės fomavimas Cyber terorizmas
Įsilaužimas į verslo sistemas Įsilaužimas į personalinius kompiuterius
Sukompromituotas pasitikėjimas e-valdžios paslaugomis R&D projektų informacijos vagystė
Diplomatinė informacija Melagingos informacijos sklaida internete Prekyba žmonėmis
Ypatingos svarbos objektų kontrolės perėmimas IPR vagystės El. špionažas
Internetinis sukčiavimas Tarptautinių org. nusikalstamų organizavimas el. priemonėmis
Įsilaužimas į išmaniuosius namus Vaikų išnaudojimas Šalies įvaizdžio kompromitavimas
Nelegalus žmogaus sekimas, informacijos rinkimas Informacijos skalidos valdymo perėmimas
El. pašto SPAM'as Nelegalių paslaugų reklama, organizavimas
Klientų informacijos vagystė Cyber karai Konfidencialios informacijos atskleidimas
Oficialių media, informacijos skalidos kanalų turinio pakeitimas Nusikaltimų įkalčiai
Prisijungimo prie finansų valdymo paslaugų vagystė
Sunkių nusikaltimų planavimas, koordinavimas, vykdymas el. priemonių pagalba
L3CE Lithuanian Cybercrime Center of Excellence
for Training, Research & Education Vidinė rinkodaros ir finansinės inf. vagystė
Teisėsaugos veiksmų sekimas, planuojamų operacijų atskleidimas

- Kaip užtikrinti valstybės ir visuomenės saugumą kibernetinėje erdvėje

Arba

- Kaip užtikrinti valstybės ir visuomenės saugumą kibernetinės erdvės pagalba

IT saugumo standartai ir sertifikacija

V•T•E	Information security certifications	[hide]
CompTIA	Security+ • CASP	
Cisco Systems	CCNA Security • CCNP Security • CCIE Security	
EC-Council	ENSA • CEH • CHFI • ECSA • LPT • CNDA • ECIH • ECSS • ECVP • EDRP • ECSP • ECSO • CJCISO	
GIAC	GSIF • GSEC • GCFW • GCIA • GCIH • GCUX • GCWN • GCED • GPEN • GWAPT • GAWN • GISP • GLSC • GCPM • GLEG • G7799 • GSSP-NET • GSSP-JAVA • GCFE • GCFA • GREM • GSE	
ISACA	CISA • CISM • CGEIT • CRISC	
(ISC) ²	SSCP • CAP • CSSLP • CISSP • ISSAP • ISSEP • ISSMP • HCISPP • CCFP	
ISECOM	OPST • OPSA • OPSE • OWSE • CTA	
Offensive Security	OSCP • OSCE • OSCP	
Juniper Networks	JNCIS Security Specialist • JNCIP Security Professional • JNCIE Security Expert	
British Computer Society	CISMP • Certificate in Business Continuity Management • Certificate in Data Protection • Certificate in Freedom of Information • Certificate in Information Risk Management • Certificate in Information Assurance Architecture	
The Open Group	Open FAIR Foundation	
Cloud Security Alliance	CCSK	
CERT	CSIH	
eLearnSecurity	eCPPT • eWPT	
PCI SSC	PCIP • QSA • PA-QSA • QSA (P2PE) • PA-QSA (P2PE) • ISA • QIR • ASV	

IT tyrimų, ekspertizės standartai ir sertifikacija

EnCE - EnCase Certified Examiner

GCFA - GIAC Certified Forensics Analyst

Q/FE - Qualified Forensics Expert

CEECS - Certified Electronic Evidence Collection Specialist Certification

CFCE - Certified Forensic Computer examiner

CCE - Certified Computer Examiner

CFE – Certification Fraud Examiner

Kibernetika policijoje

- Kibernetiniai nusikaltimai sudaro mažiau nei % (finansiniai, malware, nelegalus turinys);
- Elektroniniai įkalčiai yra surenkami ~85% visų bylų;
- Cyber Forensic specialistų yra ~ 50 (20 PD, 30 LT);
- ~15000 tyrėjų ir kitų policijos specialistų LT, kurie susiduria su elektroniniais įkalčiais;
- Kibernetinkos srityje spacializuotų prokurorų, teisėjų nėra;
- 1 tyrimų darbo vietos kaina 80-100k LTL be atlyginimų;

Pagrindinės problemos

- Dalis įkalčių nėra surenkama dėl aktyvios sistemos tyrimo žinių trūkumo;
- Tinkle reziduojantys įkalčiai nėra renkami dėl žinių trūkumo ir teisinės bazės netikslumo;
- Verslo ar su įmonėmis susijusios bylos yra šaldomos dėl kompetencijos ir technikos apribojimų;
- Dalis užklausimų specialistams yra niekiniai;
- Pilnai “rankinis” tyrimo procesas;
- Nevykdoma elektroninė žvalgyba;
- Ilgas sprendimų priėmimo procesas;
- Augantis įkalčių skaičius reikalauja daugiau darbo vietų – biudžeto nėra; 😊

Teisėsaugos kompetencijos: kodėl stringam

- Prokurorai, teisėjai:

Kriminologija, IT teisė, IT tyrimų procesas, IT tyrimų galimybės, įrodymų pakankumas ir legitimumas.

- Informacijos analitikai, žvalgybininkai:

Žvalgyba, teisinis proceso reguliavimas, asmens duomenų sauga, kompiuterinių sistemų ir tinklų inžinerijos žinios, automatizuotas duomenų rinkimas ir analizė, informacijos semantinė analizė.

- Tyrėjai, ekspertai, specialistai:

Teisinis proceso reguliavimas, asmens duomenų sauga, kompiuterinių sistemų ir tinklų inžinerijos žinios, automatizuotas duomenų rinkimas ir analizė, OS, programavimo kalbos, IT tyrimų procesas, elektroninių įrodymų surinkimas ir dokumentavimas

- Vadovai:

Kriminologija, bazinės visų IT sričių žinios, kompiuterinių resursų valdymas, kompiuterinių ar IT kompetencijų valdymas, laboratorijos organizavimas ir valdymas,

OSINT tampa pagrindinė prevencijos priemonė

- 2,4 milijardo žmonių naudoja internetą
- **Wikipedia** yra palaikoma 270 kalbų ir talpina 19 milijonų straipsnių
- **Candy Crush** žaidimus naudoja 7,6 milijonai naudotojų per dieną
- **Google** - 100 milijardų paieškos užklausų per mėnesį
- **Youtube** - įkeliamos 24 h naujos video medžiagos kas sekundę
- **Facebook**
 - 175 milijonai naudotojų yra prisijungę kiekvienu momentu
 - Kiekvienas praleidžia po 40 minučių kasdien
 - 50% mobilaus internetinio srauto (UK Stats)
- **Netflix** – 22 mln h TV ir kino medžiagos kasdien
- **Pandora** – 19 mln h muzikos kasdien
- **Zynga** – 1 petabaitas žaidimų turinio kasdien
- 4,000 naujų knygų kasdien
- **New York Times** savaitės turinys talpina informacijos tiek pat kiek 18 amžiuje žmogus sužinodavo per visą savo gyvenimą....

Iššūkiai ir galimybės

- Lietuvos resursiniai apribojimai
 - Kalbos barjeras
 - Vidinio bendradarbiavimo trūkumas
 - Barjerinės šalies pozicija
 - Nepakankamas tinklinimasis
 - Tardisciplininio mokymo programų trūkumas
-
- Turim didelį kalbinį potencialą
 - Turėjom stiprią žvalgybos mokyklą
 - Turim gerą analitikos mokyklą

Galimi sprendimai, kitų šalių praktikos

- Pagrindiniai įrankiai – open source pagrindu
- Visoms technologijoms sprendimų sukūrimas yra neįmanomas, dėl to darbo organizavimas paremtas analitinėmis metodikomis ir priemonėmis:
 - Virš 100 operacinių sistemų
 - Virš 700 programavimo kalbų
- Kompetencijų kūrimas paremtos laboratorijomis
- Kompetencija yra vystoma partnerystės pagrindu

Bendradarbiavimo link

- Lietuvos akademinės bendruomenės atstovai pasitelkdami tarptautinius, verslo ir privačius partnerius bei bendradarbiaudami su teisėsaugos institucijų atstovais įkūrė L3CE (“Lietuvos kibernetinių nusikaltimų kompetencijų ir tyrimų centrą”).
- L3CE misija ir tikslai:
 - Kurti mokymų programas pagal Europolo bei kitų ES institucijų patvirtintas metodikas ir standartus;
 - Organizuoti mokymus elektroninės informacijos saugos ir elektroninių nusikaltimų srityse;
 - Vykdyti mokslinius tyrimus kibernetinio saugumo tema;
 - Tarp centrų ir teisėsaugos institucijų nemokamai keistis mokymo programomis, įrankiais, ekspertais;
 - Surinkti ir konsoliduoti poreikį mokymams;
 - Organizuoti tarptautinius renginius skirtus teisėsaugos pareigūnams; kibernetinė saugos bei nusikaltimų tyrimo temomis;
 - Sukurti bei palaikyti bendrą žinių ir ekspertų duomenų bazę;
 - Kurti įrankius, reikalingus teisėsaugos pareigūnams kovai su nusikaltimais elektroninėje erdvėje;
 - Bendradarbiauti su ECTEG (European cybercrime training and education group) ir EC3 (European cybercrime centre, Europol);
- L3CE priklauso Europos kibernetinių nusikaltimų ir kibernetinio saugumo kompetencijų centrų tinklui;

L3CE vystymo projektas

- **Projekto pavadinimas:**

Lithuanian Cybercrime Centre of Excellence for Training, Research & Education (L3CE)

Lietuvos kibernetinių nusikaltimų kompetencijų, tyrimų ir švietimo centro kūrimas

- **Pareiškėjas:** Lietuvos kibernetinių nusikaltimų kompetencijų ir tyrimų centras

- **Projekto partneriai:** MRU, KTU, UCD, Madrido autonominio universitetas, Vilniaus AVPK ir kiti.

- **Finansavimo programa:** EC DG Home Affairs ISEC programa (Prevention of and against crime 2007-2013), tema - Illegal Use of Internet

- **Projekto biudžetas:** ~1MEU

- **Trukmė:** 18 mėn.

- **Projekto uždaviniai:**

- L3CE steigimas, plėtra ir tarptautinis bendradarbiavimas
- 5 Mokymų programos
- Kriminalistikos atviro kodo įrankių laboratorija (Forensic Open Source Tools)
- 1 Sertifikavimo programa

Specialistų pritraukimas ir išlaikymas

- Privačios rinkos ir teisėsaugoje dirbančių specialistų atlyginimai yra nepalyginami

Average Base Salary



Apibendrinimai

- Sąvalaikis kompetencijų ugdymas yra įmanomas tik bendradarbiaujant su kitų šalių švietimo institucijomis, tarptautiniais kompetencijų tinklais.
- Norint būti lygiaverčiu partneriu tarptautinėje kiber-saugos bendruomenėje, reikia specializuotis ir gerai išmanyti bent vieną sritį.
- Turi būti išvystyta ir reglamentuota kyber-saugos kompetencijų struktūra bei pripažinimo mechanizmai.
- Turi būti tokia DU struktūra, kuri leistų išlaikyti specialistus bent jau iki rinkos vidurkio (IT darbuotojų kaitos ciklas – 3-5 metai).
- Kiber-saugos kompetencijos turi būti adaptuotos ir vystomos atsižvelgiant į Lietuvos ir regiono specifiką.
- Didžiausios grėsmės išlieka informacijos manipuliavimo, propogandos ir informacinio karo srityse, privaloma stiprinti kiber-žvalgybines kompetencijas.
- Provaloma tarpinstitucinė poreikių konsolidacija, siekiant užtikrinti pakankamą specializaciją bei pasinaudojant kitais masto ekonomikos teikiamais pranašumais.