PERSONAL INFORMATION

Lect. dr. ing. PUNCIOIU Alin-Marian (*CISSP, CEH, CHFI, GWAPT, GREM, GRID, GNFA, OSCP, Change Management Practitioner, QRadar Analyst*)

Academia Tehnică Militară, Bd. George Coşbuc Nr. 39-49 , 050141, Bucureşti, România

0743183383

alin.puncioiu@mta.ro

Naționalitate Română

EXPERIENŢA PROFESIONALĂ

Experienţa profesională

Perioada **2018 – Prezent**

Funcţia sau postul ocupat: Lector Universitar

Activităţi şi responsabilităţi principale:
- Susţinerea de activităţi didactice la disciplinele: Securitate informatică, Elemente de Securitate cibernetică, Managementul securității informațiilor/ sistemelor informatice, Criminalitatea informatică, colectarea şi investigarea probelor, Război cibernetic, Securitatea sistemelor de operare, Logistica sistemelor și echipamentelor de calcul, Monitorizarea securității sistemelor și raportarea incidentelor de securitate

Numele şi adresa angajatorului: Academia Tehnică Militară, Bd. George Coşbuc Nr. 39-49, 050141, Bucureşti, România

Tipul activităţii sau sectorul de activitate: Învățământ

Perioada **2022 – Present**

Funcţia sau postul ocupat: Specialist în securitate cibernetică

Activităţi şi responsabilităţi principale:
- Coordonarea echipei de răspuns rapid și unitar la incidente de securitate cibernetice;
- Investigarea incidentelor de securitate cibernetică şi analiza mostrelor de malware identificate în cadrul analizelor informatice desfășurate;
- Elaborarea şi/sau actualizarea politicilor şi procedurilor de securitate în domeniul securității cibernetice;
- Asigurarea prevenirii, detectării şi răspunsului la incidentele de securitate cibernetice prin monitorizarea diferitelor rețele de sisteme informatice folosind aplicații specifice şi echipamente de analiză și investigare incidente de securitate cibernetică.

Numele şi adresa angajatorului: Happening Technologies

Tipul activităţii sau sectorul de activitate: Securitate cibernetică, Răspuns la incidente cibernetice

Perioada **2016 – 2021**

Funcţia sau postul ocupat: Specialist în securitate cibernetică

Activităţi şi responsabilităţi principale:
- Coordonarea unor echipe de specialiști pentru asigurarea răspunsului rapid și unitar la incidente de securitate cibernetice atât în medii tradiționale de IT cât și ăn medii de control industrial (SCADA/ OT);
- Investigarea incidentelor de securitate cibernetică şi analiza mostrelor de malware identificate în cadrul analizelor informatice desfășurate;
- Elaborarea şi/sau actualizarea politicilor şi procedurilor de securitate în domeniul securității cibernetice;
- Asigurarea prevenirii, detectării şi răspunsului la incidentele de securitate cibernetice prin monitorizarea diferitelor rețele de sisteme informatice folosind aplicații specifice şi echipamente de analiză și investigare incidente de securitate cibernetică.

Numele şi adresa angajatorului: DELL Secureworks

Tipul activităţii sau sectorul de activitate: Securitate cibernetică, Răspuns la incidente cibernetice

Perioada **2006 – 2016**

Funcţia sau postul ocupat: Ofiţer – Specialist în cadrul Centrului Tehnic Principal - CERTMIL/ MApN

Activităţi şi responsabilităţi principale	• Investigarea incidentelor de securitate cibernetică şi analiza mostrelor de malware identificate în cadrul analizelor informatice desfăşurate; • Elaborarea şi implementarea politicilor şi procedurilor de securitate în domeniul securităţii cibernetice din M.Ap.N.; • Participarea la activităţi de prevenire, detectare şi răspuns la incidentele de securitate cibernetice prin monitorizarea reţelei locale folosind aplicaţii specifice şi echipamente de analiză şi investigare incidente de securitate cibernetică; • Reprezentarea națională și internațională a MApN în cadrul exercițiilor de apărare cibernetică; • Responsabilităţi în dezvoltarea, implementarea, integrarea reţelelor de calculatoare şi suport pentru utilizatorii acestora; • Responsabilităţi în dezvoltarea şi securizarea de aplicaţii web; • Responsabilităţi în identificarea şi minimizarea riscurilor şi vulnerabilităţilor identificate/ semnalate în sistemele informatice şi de comunicaţii; • Instalare, configurare şi administrare echipamentelor de reţea şi a servere-lor din cadrul organizaţiei.
Numele şi adresa angajatorului	Ministerul Apărării Naționale
Tipul activităţii sau sectorul de activitate	Securitate cibernetică, IT - Securitatea informației
Perioada	**2014-2015**
Funcţia sau postul ocupat	Cadru didactic asociat
Activităţi şi responsabilităţi principale	• Susţinerea de activităţi didactice la disciplina Securitate militară
Numele şi adresa angajatorului	Academia Forţelor Terestre „Nicolae Bălcescu”, str. Revoluţiei, nr. 3-5, Sibiu, România.
Tipul activităţii sau sectorul de activitate	Învățământ.
Perioada	**2013-2015**
Funcţia sau postul ocupat	Şef echipă tehnică în proiectul „*Sistem naţional de protecţie a infrastructurilor IT&C de interes naţional împotriva amenințărilor provenite din spaţiul cibernetic”*
Activităţi şi responsabilităţi principale	Implementarea unor componente informatice de securitate destinate protecţiei sistemelor informatice şi de comunicaţii şi informaţiilor vehiculate la 6 instituţii publice beneficiare.
Numele şi adresa angajatorului	Ministerul Apărării Naţionale în parteneriat cu Serviciul Român de Informaţii
Tipul activităţii sau sectorul de activitate	Securitate/apărare cibernetică.
Perioada	**2013-2015**
Funcţia sau postul ocupat	Expert în proiectul „*Advanced Cyber Defence Centre (ACDC)”*
Activităţi şi responsabilităţi principale	- realizarea de activități de cercetare științifică în domeniul tehnicilor și metodelor de combatere a rețelelor de tip Botnet - documentarea, instalarea și configurarea unor sisteme informatice destinate identificării de atacuri cibernetice asupra domeniilor web, implementarea şi integrarea acestora în cadrul infrastructurii cibernetice creată; - documentarea, instalarea și configurarea unor sisteme automate de analiză a mostrelor de malware colectate în cadrul proiectului.
Numele şi adresa angajatorului	Centrul Naţional de răspuns la incidente de securitate cibernetică - CERT-RO, B-dul Mareşal Averescu, nr. 8-10, Sector 1, Bucureşti.
Tipul activităţii sau sectorul de activitate	Securitate cibernetică. Combaterea amenințărilor cibernetice.

EDUCAŢIE ŞI FORMARE

Perioada	**Dec. 2017 – Ian. 2018**
Calificarea / diploma obţinută	Offensive Security Certified Proffessional
Disciplinele principale studiate / competenţe profesionale dobândite	Identificarea și exploatarea vulnerabilităților existente într-un laborator informatic.
Numele şi tipul instituţiei de învăţământ / furnizorului de formare	Offensive Security
Perioada	**Sep. 2017**
Calificarea / diploma obţinută	Diplomă de participare la cursul Situational Leadership: Building Leaders
Disciplinele principale studiate / competenţe profesionale dobândite	Situational Leadership este un instrument puternic, dar flexibil, care permite liderilor acumularea de cunoștințe pentru a influența mai eficient persoanele cu care interacționează.
Numele şi tipul instituţiei de învăţământ / furnizorului de formare	The Center for Leadership Studies
Perioada	**Apr. 2017 – Iulie 2017**
Calificarea / diploma obţinută	Diplomă de participare la cursul Business Relationship Management

Disciplinele principale studiate / competenţe profesionale dobândite	Abordare formală pentru înțelegerea, definirea și susținerea activităților în mediul de lucru. Cursul prezintă cunoștințe, abilități și comportamente (sau competențe) care promovează o relație productivă între o organizație și partenerii lor de afaceri.
Numele şi tipul instituţiei de învăţământ / furnizorului de formare	Serious Consulting
Perioada	**2011 – 2015** (şedinţă publică 29.09.2015)
Calificarea / diploma obţinută	Diplomă de doctor
Disciplinele principale studiate / competenţe profesionale dobândite	Inginerie mecanică
Numele şi tipul instituţiei de învăţământ / furnizorului de formare	Şcoala Doctorală din Academia Tehnică Militară – Bucureşti
Perioada	**25-30.05.2015**
Calificarea / diploma obţinută	SANS GIAC Reverse Engineering Malware (GREM) | GIAC GREM Certification
Disciplinele principale studiate / competenţe profesionale dobândite	Securitate cibernetică, analiză de malware, statică și dinamică, Reverse Engineering, dezasamblare și debugging cod malware
Numele şi tipul instituţiei de învăţământ / furnizorului de formare	SANS Information Security Training
Perioada	**19-23.01.2015**
Calificarea / diploma obţinută	SANS GWAPT(Web App Pentesting) | GIAC Web Application Penetration Tester (GWAPT) certification
Disciplinele principale studiate / competenţe profesionale dobândite	Arhitectura aplicaţiilor web, etapele parcurse în desfăşurarea testelor de penetrare a aplicaţiilor web, tehnici de exploatare a aplicaţiilor web, instrumente software utilizate.
Numele şi tipul instituţiei de învăţământ / furnizorului de formare	SANS Information Security Training
Perioada	**27–31.10.2014**
Calificarea / diploma obţinută	Certified Information System Security Professional
Disciplinele principale studiate / competenţe profesionale dobândite	Securitatea echipamentelor şi reţelelor, Managementul riscului de securitate, evaluări şi testări de securitate, asigurarea securităţii cibernetice în organizaţii
Numele şi tipul instituţiei de învăţământ / furnizorului de formare	The International Information System Security Certification Consortium
Perioada	**07.07-19.09.2014**
Calificarea / diploma obţinută	Diplomă de participare la cursul "*Cyber security – Vulnerability Assessment and Certified Ethical Hacker Course (CEH)*"
Disciplinele principale studiate / competenţe profesionale dobândite	Securitate cibernetică, evaluarea vulnerabilităţilor reţelelor, amprentarea şi recunoaşterea reţelelor, scanarea şi enumerarea serviciilor, instrumente şi tehnici de atac informatic, inginerie socială, deturnarea sesiunilor, exploatarea aplicaţiilor web, sisteme honeypots.
Numele şi tipul instituţiei de învăţământ / furnizorului de formare	Naval Postgraduate School, Monterey, California
Perioada	**07– 11.04.2014**
Calificarea / diploma obţinută	Certifiat de participare la cursul Advanced Malware Analysis
Disciplinele principale studiate / competenţe profesionale dobândite	Securitate cibernetică, analiză de malware, statică și dinamică, Reverse Engineering, dezasamblare și debugging cod malware
Numele şi tipul instituţiei de învăţământ / furnizorului de formare	MANDIANT, a FireEye Company
Perioada	**03-07.03.2014**
Calificarea / diploma obţinută	Computer hacking forensic investigation / C|HFI certification
Disciplinele principale studiate / competenţe profesionale dobândite	Securitate cibernetică, securitatea sistemelor informatice și de comunicații, investigații informatice, probe digitale, răspuns la incidente cibernetice
Numele şi tipul instituţiei de învăţământ / furnizorului de formare	EC- Council
Perioada	**19.08.2013 – 27.09.2013**

Calificarea / diploma obţinută	Certificat de participare la Cyber Security Short Course
Disciplinele principale studiate / competenţe profesionale dobândite	Securitate cibernetică, securizare și administrare reţea, investigare incidente cibernetice, analiză trafic de rețea
Numele şi tipul instituţiei de învăţământ / furnizorului de formare	Naval Postgraduate School, Monterey, California
Perioada	**2010 – 2012**
Calificarea / diploma obţinută	Studii universitare de masterat / Diplomă de master
Disciplinele principale studiate / competenţe profesionale dobândite	Inginerie şi Management, Ştiinţe ale Educaţiei
Numele şi tipul instituţiei de învăţământ / furnizorului de formare	Universitatea Tehnica de Construcţii Bucureşti – Departamentul de Pregătire al Cadrelor Didactice
Perioada	**2007 – 2010**
Calificarea / diploma obţinută	Licenţiat în informatică / Diplomă de licenţă
Disciplinele principale studiate / competenţe profesionale dobândite	Informatică – limbaje de programare - baze de date şi administrare reţea
Numele şi tipul instituţiei de învăţământ / furnizorului de formare	Universitatea din Bucureşti – Facultatea de Matematică – Informatică
Perioada	**2007 – 2009**
Calificarea / diploma obţinută	Studii postuniversitare / Diplomă de studii postuniversitare de specializare
Disciplinele principale studiate / competenţe profesionale dobândite	Informatică – reţele – programare
Numele şi tipul instituţiei de învăţământ / furnizorului de formare	Universitatea Tehnică de Construcţii Bucureşti – Departamentul de Pregătire al Cadrelor Didactice
Perioada	**2001 – 2006**
Calificarea / diploma obţinută	Inginer
Disciplinele principale studiate / competenţe profesionale dobândite	Matematică – Fizică – Inginerie Mecanică
Numele şi tipul instituţiei de învăţământ / furnizorului de formare	Academia Tehnică Militară, Facultatea de Mecatronică şi Sisteme Integrate de Armament

Lucrări didactice	*Sisteme de alertă timpurie – HONEYPOTS*, Editura Academiei Tehnice Militare, București, 2018, ISBN 978-973-640-282-1
Lucrări științifice publicate și susținute la conferințe internaționale	Publicații în jurnale indexate în baze de date internaționale recunoscute și reviste tehnice de specialiate Speaker la conferința internalionala DefCamp 2016, cu prezentarea ***Blitzkrieg malware analysis*** Speaker la conferința internalionala DefCamp 2017, cu prezentarea ***Fileless malware – beyond a cursory glance***