Daniel Pănescu

dppanescu@gmail.com   0725996407

linkedin.com/in/daniel-panescu   https://danielpanescu.tk

Summary

I am a skilled Cyber Security Analyst with over 3 years of experience in the field and an additional 7 years of experience in Networking and Communication. My background includes working in a military environment and participating in national and international exercises and missions. I have a strong track record of success in monitoring, detecting, analyzing, and threat hunting, as well as expertise in SIEM (Security Information and Event Management) analysis using tools such as ArcSight, Splunk, QRadar, Wazuh, and ElasticSearch.

My experience extends to a variety of security solutions, including Intrusion Prevention Systems (NSP McAfee IDS/IPS), Firewalls (Fortigate, Palo Alto, Cisco ASA, OPNsense, PfSense), Web Application Firewalls (FortiWeb, Radware Appwall), Email Gateways (Cisco Email Security Appliance, FortiMail), Web Proxies (Cisco Web Security Appliance, Squid), Email Security (FireEye EX, Threat Grid, Advanced Malware Protection), Network Security (FireEye NX), SOAR (Palo Alto Cortex XSOAR, Splunk Phantom), Full Packet Capture (Moloch/Arkime), SIRP (The Hive Project, Corbex), Sharing Platforms (MISP, OpenCTI), Vulnerability Assessment (Tenable SC/Nessus, AppScan, Acunetix), Anti-Virus (Bitdefender Gravity Zone), Endpoint Detection and Response (Bitdefender Gravity Zone), and Data Loss Prevention (McAfee).

Experience

Cyber Security Analyst

Ministerul Apararii Nationale

Apr 2019 - Present (3 years 10 months)

As a Cybersecurity professional, my main responsibility is to protect sensitive or confidential information from unauthorized access or use. This includes identifying and assessing potential security risks, designing and implementing security controls to mitigate those risks, and monitoring systems for unusual activity. I use a variety of tools and techniques to accomplish this, such as Intrusion Prevention Systems, Firewalls, Web Application Firewalls, Email Gateways, Web Proxies, Network Security solutions, Vulnerability Assessment tools, and Endpoint Detection and Response solutions. I also perform regular vulnerability assessments and penetration testing to identify and remediate vulnerabilities in the organization's systems and networks.

In the event of a security incident, I follow incident response procedures to contain and remediate the issue, and then document and analyze the incident to identify the root cause and improve overall security. I also stay up to date with the latest cybersecurity trends and threats, and recommend and implement security best practices to improve the organization's overall security posture. Additionally, I work closely with the security operations team to design and implement security monitoring solutions such as SIEM, SOAR, and Full Packet Capture to detect and respond to security incidents in a timely and effective manner.

Web Developer

Freelance

Sep 2018 - Present (4 years 5 months)

As a software developer, responsibilities include writing well-designed, testable, and efficient code using best practices, creating website layouts and user interfaces using standard HTML/CSS, integrating data from various back-end services and databases, gathering and refining specifications and requirements based on technical needs, creating and maintaining software documentation, maintaining, expanding, and scaling our site, staying informed of emerging technologies and industry trends and applying them to operations and activities, and working with web designers to match visual design intent

Security Administrator
Ministerul Apararii Nationale
Sep 2018 - Apr 2019 (8 months)
Installing, administering and troubleshooting network security solutions, updating software with the latest security patches, creating network policies and authorization roles, defending against unauthorized access, modifications and destruction, consulting with staff, managers and executives about the best security practices and providing technical advice, configuring and supporting security tools such as firewalls and anti-virus software, training staff to understand and use security protocols, performing vulnerability and penetration tests, identifying and defending against threats, developing disaster recovery plans, configuring security systems, analyzing security requirements, recommending improvements and monitoring network traffic for suspicious behavior.

Network Administrator
Ministerul Apararii Nationale
Apr 2016 - Sep 2018 (2 years 6 months)
Designing, installing, and managing network infrastructure, ensuring functionality of computer networks and connection/communication equipment, server administration, identifying and resolving network and system issues, consulting with clients to specify requirements and design solutions, budgeting for equipment and assembly costs, assembling new systems, maintaining existing software/hardware and upgrading as needed, monitoring networks to improve performance, working with IT support personnel, and providing network administration and support.

System Administrator
Ministerul Apararii Nationale
Nov 2015 - Apr 2016 (6 months)
As an IT professional, I am responsible for installing and configuring software and hardware, managing network servers and technology tools, setting up accounts and workstations, monitoring performance and maintaining systems according to requirements, troubleshooting issues and outages, ensuring security through access controls, backups and firewalls, upgrading systems with new releases and models, developing expertise to train staff on new technologies, and building an internal wiki with technical documentation, manuals and IT policies.

Education

Universitatea „Spiru Haret" din București
Bachelor's degree, Engineering and Computer Science
Oct 2017 - Present
The study and application of programming languages, software development methodologies, and computer systems architecture to design, build, and maintain software applications. This includes in-depth understanding of data structures, algorithms, and software design patterns, as well as proficiency

in database management systems, network infrastructure, and project management. Additionally, the program covers the theoretical foundations of computer science, such as formal models, automata theory, and computational complexity, and the use of these concepts to analyze and optimize software systems. Graduates of this program will have a comprehensive understanding of the principles and practices of computer science and the ability to apply them in a professional setting.
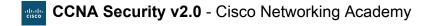
Military School of Communications, Information Technology and Cyber Defense
Gruaduation Diploma, Computer Systems Networking and Telecommunications
Aug 2013 - Aug 2015
As a graduate of a military IT specialist school, I received specialized training in the operation, maintenance and administration of military communications technology and IT equipment, including systems and networks. My training covered a wide range of topics, including IT and cyber security, communications systems and networks administration, and the use of communications equipment and techniques in military operations. Additionally, I gained expertise in the management of micro-structures at crew, group, and unit level, as well as cyber defense. My training also included training as a military specialist in the field of systems security administration, communications networks and computer science. I have the skills and knowledge to ensure the smooth operation and maintenance of equipment and communications equipment in various military scenarios.

Licenses & Certifications

CCNA: Introduction to Networks - Cisco

Introduction to Cybersecurity - Cisco

CCNA: Switching, Routing, and Wireless Essentials - Cisco

Cybersecurity Essentials - Cisco

Network Defense - Cisco

Cyber Threat Management - Cisco

Endpoint Security - Cisco

Python Essentials 1 - Cisco

AWS Well - Architected - Amazon Web Services (AWS)
E-03M461

Introduction to IoT - Cisco

CCNA Security v2.0 - Cisco Networking Academy

Cybersecurity Pathway - Cisco

Skills

Amazon Web Services (AWS) • IT Operations • Python (Programming Language) • Linux • Bash • Windows Server • Cybersecurity • Linux System Administration • Cyber Threat Intelligence (CTI) • Vulnerability Management