europass

Vlad Mihai Ursache

Email: ursachevladmihai@yahoo.com

Website: https://www.researchgate.net/profile/Vlad-Ursache-2?ev=hdr_xprf

Gender: Male **Date of birth:** 21/11/1984 **Place of birth:** Romania **Nationality:** Romanian

WORK EXPERIENCE

Overall experience

With more than 12 years of professional experience in information technology and cybersecurity, complemented by a Master's degree in Advanced Computer Science, I have built and led cybersecurity capabilities that strengthen organizational resilience, improve operational maturity, and enable secure digital transformation. My expertise spans cybersecurity strategy, Security Operations Centers (SOC), SIEM, XDR, XSIAM, XSOAR, cyber defense, governance, regulatory compliance, security operations, policy development, and enterprise risk management.

Beyond technical expertise, I bring proven leadership and management experience. For over three years, I have led multidisciplinary cybersecurity teams and managed technical workgroups, driving operational excellence, mentoring cybersecurity professionals, coordinating cross-functional initiatives, and ensuring the successful delivery of strategic security programs. My management approach combines technical excellence, business alignment, stakeholder engagement, and continuous improvement to achieve measurable organizational outcomes.

Throughout my career, I have worked closely with executive leadership, and senior decision-makers across both public and private sectors to translate complex cybersecurity challenges into strategic business initiatives. I have successfully led customer engagements, directed complex security projects, contributed to cybersecurity strategy and service development, and delivered secure onboarding programs for organizations operating diverse technologies, regulatory environments, and business requirements.

My technical background is supported by extensive experience in cybersecurity operations, incident response, vulnerability management, threat detection and hunting, network security, internal auditing, Zero Trust principles, and cybersecurity governance. I also possess practical expertise in Artificial Intelligence, Large Language Models (LLMs), Python, TensorFlow, and the application of AI to modern cybersecurity operations, enabling the integration of intelligent automation and advanced analytics into security programs.

In addition to my professional responsibilities, I have actively contributed to the advancement of cybersecurity at both national and European levels. As a volunteer with Romania's National Cyber Security Directorate (DNSC), I have participated in initiatives supporting the implementation of the Cybersecurity Act, the NIS Directive, GDPR, the European Data Strategy, and cybersecurity capability and capacity-building programs. These activities have strengthened collaboration between government institutions, industry, and academia while supporting the development of resilient cybersecurity ecosystems.

I am also an active contributor to several European and international cybersecurity and technology working groups through DNSC, ISACA, and other professional associations. My work focuses on cybersecurity governance, international cooperation, information sharing, trust-building, strategic policy development, emerging technologies, and the advancement of cyber resilience across public and private sectors.

My professional objective is to bridge executive leadership, cybersecurity strategy, Artificial Intelligence, and academic research to help organizations and governments build resilient, secure, and future-ready digital ecosystems while fostering innovation, operational excellence, and sustainable cyber resilience.

SNTGN Transgaz SA

City: Medias | **Country:** Romania

[01/12/2025 – Current] **Senior Compliance Manager**

Key Responsibilities and Leadership Contributions

- Led cybersecurity governance, compliance, and risk management initiatives, ensuring organizational alignment with **ISO/IEC 27001**, the **NIS Directive/NIS2**, cybersecurity regulations, internal policies, and industry best practices.
- Served as a trusted advisor to executive leadership, project managers, and technical teams on cybersecurity governance, regulatory compliance, information security strategy, risk mitigation, and security program maturity.
- Managed compliance activities across multiple customer engagements, including security assessments, control implementation, gap analysis, audit preparation, remediation planning, compliance reporting, and continuous improvement of Information Security Management Systems (ISMS).
- Coordinated cross-functional teams to develop, implement, and maintain security policies, standards, procedures, governance frameworks, and compliance documentation supporting organizational objectives and regulatory obligations.
- Conducted enterprise cybersecurity risk assessments, project risk evaluations, and security reviews, identifying strategic risks, recommending mitigation measures, and supporting executive decision-making through risk-based analysis.
- Led customer onboarding activities for complex cybersecurity programs, ensuring secure integration of diverse technologies, operational processes, regulatory requirements, and business objectives.
- Collaborated closely with CIOs, CISOs, security architects, infrastructure teams, governance leaders, auditors, and external stakeholders to strengthen cybersecurity posture and ensure effective governance across enterprise environments.
- Managed incident response processes, developing incident handling procedures, escalation workflows, operational playbooks, automation requirements, and technical documentation to improve response consistency, resilience, and service quality.
- Worked closely with CSIRC, DFIR teams, Threat Intelligence, infrastructure engineers, cloud specialists, and external partners to validate incident response coverage, enhance operational readiness, and improve cross-team collaboration.
- Managed enterprise vulnerability management programs using **Rapid7 InsightVM,** prioritizing remediation based on business risk, exploitability, asset criticality, and customer-specific operational requirements while providing strategic remediation recommendations.
- Applied expertise in Artificial Intelligence, Large Language Models (LLMs), Python, and automation technologies to enhance cybersecurity operations, improve analytical capabilities, and support intelligent security process optimization.
- Participation in Cyber Security National Exercise (Cydex 2025) organized by National Cyberint Center, Romanian intelligence Service (SRI)

SNTGN Transgaz SA

City: Medias | **Country:** Romania

[03/01/2023 – 01/12/2025] **Senior Cybersecurity Expert**

Key Responsibilities and Strategic Contributions

- Provided senior level cybersecurity expertise and strategic advisory services to public and private sector organizations, strengthening cyber resilience, reducing organizational risk, and enabling secure digital transformation initiatives.
- Served as a trusted advisor to executive leadership, translating complex cybersecurity risks into strategic recommendations, governance frameworks, and business-aligned security initiatives.
- Led the design, implementation, and continuous improvement of enterprise cybersecurity programs, integrating governance, risk management, compliance, security operations, and modern cyber defense capabilities aligned with organizational objectives.
- Directed cybersecurity assessments, security architecture reviews, and technical risk analyses across on-premises, cloud, and hybrid infrastructures, identifying critical vulnerabilities and recommending pragmatic, risk-based remediation strategies.
- Managed the full incident response lifecycle, including preparation, detection, triage, containment, eradication, recovery, post-incident analysis, lessons learned, and continuous process improvement in accordance with international cybersecurity best practices.
- Developed advanced SIEM content, dashboards, correlation searches, detection analytics, and security automation using **Rapid7**, and other enterprise security platforms, enabling proactive detection of sophisticated cyber threats.
- Led enterprise vulnerability management initiatives utilizing **Rapid7 InsightVM, Nessus,** prioritizing remediation activities based on exploitability, business impact, asset criticality, and organizational risk appetite while advising stakeholders on strategic remediation planning.
- Strengthened cloud security and identity governance by supporting secure implementations across organization.
- Contributed to cybersecurity governance by developing security policies, operational procedures, technical standards, security baselines, and documentation aligned with **ISO/IEC 27001**, **NIS2**.
- Contributed to the continuous improvement of cybersecurity maturity through strategic planning, capability development, operational optimization, security awareness, and the adoption of emerging technologies and industry best practices.
- Selected to participate in the CYDEX National Cyber Security Exercises (2023 and 2024), organized by the National Cyberint Center of the Romanian Intelligence Service (SRI), collaborating with cybersecurity professionals in realistic cyber-attack simulation scenarios designed to enhance national cyber resilience, incident response coordination, inter-agency collaboration, and critical infrastructure protection.

National Cyber Security Directorate (DNSC)

City: Bucharest | **Country:** Romania

[28/03/2021 – 03/01/2023] **Volunteer Cybersecurity Expert**

Key Responsibilities

- Volunteered with the **National Cyber Security Directorate (DNSC)** to support national and European cybersecurity initiatives aimed at strengthening cyber resilience, promoting secure digital transformation, and enhancing cooperation between government, academia, industry, and international partners.
- Contributed to working groups and strategic initiatives focused on the implementation and adoption of European cybersecurity legislation and regulatory frameworks, including the **NIS Directive/NIS2**, the **Cybersecurity Act**, **GDPR**, the **European Data Strategy**, and emerging cybersecurity policies.
- Participated in the development, review, and discussion of cybersecurity policies, governance frameworks, best practices, and strategic recommendations supporting national cyber resilience and regulatory compliance.

- Supported cybersecurity capability and capacity building initiatives by contributing technical expertise, sharing operational experience, and promoting the adoption of modern cybersecurity practices across public and private sector organizations.
- Collaborated with cybersecurity professionals, government institutions, academic organizations, industry experts, and international partners to strengthen information sharing, trust, and coordinated responses to emerging cyber threats.
- Contributed to national and European discussions on cyber resilience, critical infrastructure protection, incident response readiness, cyber risk management, and the future evolution of cybersecurity governance.
- Participated in professional working groups, workshops, conferences, and collaborative initiatives focused on cybersecurity strategy, digital trust, emerging technologies, Artificial Intelligence, and secure digital innovation.
- Assisted in evaluating cybersecurity challenges, identifying strategic priorities, and providing practical recommendations to improve organizational and national cybersecurity maturity.
- Promoted knowledge exchange and cybersecurity awareness by sharing operational best practices, lessons learned, and practical expertise gained from enterprise security operations, incident response, threat detection, and governance.
- Supported initiatives encouraging stronger collaboration between academia, government, and industry to foster cybersecurity research, workforce development, innovation, and professional skills development.
- Contributed to discussions on international cybersecurity cooperation, cyber diplomacy, information exchange mechanisms, and the development of resilient cybersecurity ecosystems across the European Union.

I'm still maintaining contact with the DNSC as an ex-volunteer and have been included in an internal group. If a recommendation letter is required, it may be provided and signed by the General Director, Mr. Dan Cimpean.

SNTGN TRANSGAZ S.A.

City: Medias | **Country:** Romania

[31/07/2020 – 30/12/2022] **Cybersecurity Expert**

Key Responsibilities and Strategic Contributions

- Monitored and protected enterprise network infrastructures through continuous security monitoring, leveraging automated detection technologies and complementary security solutions to identify, analyze, and respond to cyber threats while ensuring the confidentiality, integrity, and availability of critical business systems.
- Conducted comprehensive internal and external network security assessments, vulnerability scanning, and asset discovery to identify security weaknesses, maintain an accurate security posture, and support proactive risk reduction across complex IT environments.
- Performed vulnerability analysis, validation, prioritization, and lifecycle management by assessing exploitability, business impact, asset criticality, and emerging threat intelligence to enable effective, risk-based remediation strategies.
- Executed **White Box** and **Gray Box Penetration Tests** to evaluate the effectiveness of security controls, identify exploitable vulnerabilities, validate defensive mechanisms, and provide actionable recommendations to improve organizational resilience.
- Performed cybersecurity risk assessments and security control evaluations to identify strategic and operational risks, supporting informed decision-making and the continuous improvement of enterprise cybersecurity maturity.
- Monitored the implementation and effectiveness of information security policies, standards, procedures, and operational processes, ensuring alignment with organizational objectives, security best practices, and regulatory requirements.
- Supported the development and continuous improvement of Information Security Management Systems (ISMS) by aligning internal security policies and technical

controls with European and national cybersecurity legislation, including the **NIS Directive**, while promoting regulatory compliance and governance excellence.
- Collaborated with infrastructure teams, system administrators, network engineers, and management to strengthen security architecture, improve defensive capabilities, and implement security-by-design principles across enterprise environments.
- Produced detailed technical assessments, vulnerability reports, risk analyses, and executive recommendations, enabling stakeholders to prioritize remediation activities and strengthen organizational cyber resilience.
- Contributed to the continuous enhancement of organizational cybersecurity capabilities by promoting security awareness, operational best practices, secure configuration standards, and continuous risk monitoring.
- Selected to participate in the CYDEX National Cyber Security Exercises (2021 and 2022), organized by the National Cyberint Center of the Romanian Intelligence Service (SRI), collaborating with cybersecurity professionals in realistic cyber-attack simulation scenarios designed to enhance national cyber resilience, incident response coordination, inter-agency collaboration, and critical infrastructure protection.

SNTGN TRANSGAZ S.A.

City: Medias | **Country:** Romania

[31/05/2015 – 31/07/2019]

RRM Administrator | Regulatory Data Reporting & Energy Market Compliance Specialist

Key Responsibilities and Strategic Contributions

- Appointed as **Registered Reporting Mechanism (RRM) Administrator** for SNTGN Transgaz S.A., responsible for the governance, operation, security, and reliability of regulatory reporting processes in direct coordination with the **Agency for the Cooperation of Energy Regulators (ACER)**.
- Managed the end-to-end reporting lifecycle for regulatory data submitted to ACER's data collection systems, ensuring accuracy, integrity, availability, confidentiality, and compliance with European energy market transparency requirements.
- Administered internal RRM processes, including system analysis, data validation, reporting workflows, operational procedures, and continuous improvement activities to ensure reliable and compliant data exchange with European regulatory platforms.
- Performed assessments of internal systems, operational capabilities, cybersecurity risks, vulnerabilities, and data protection requirements affecting regulatory reporting processes, supporting secure and resilient reporting infrastructure.
    - Ensured implementation and operational compliance with key European regulatory frameworks, including: Regulation (EU) No. 1227/2011 (REMIT) and Regulation (EU) No. 1348/2014.
- Coordinated with technical teams, business stakeholders, and regulatory representatives to ensure the successful collection, validation, processing, and transmission of energy market data required by European regulatory authorities.
- Supported data governance initiatives by establishing reporting controls, improving data quality management, ensuring traceability of submitted information, and maintaining compliance with regulatory reporting obligations.
- Analyzed internal IT systems and business processes supporting regulatory reporting, identifying potential risks, operational gaps, and improvement opportunities to enhance reliability and security.
- Collaborated within European working groups organized by the **European Network of Transmission System Operators for Gas (ENTSOG)**, contributing to discussions related to European network codes, market transparency, operational processes, and regulatory harmonization.
- Participated in international conferences, workshops, and professional working groups in **Brussels, Ljubljana, and Bucharest**, engaging with European energy institutions, industry representatives, and regulatory stakeholders.

- Supported cross-border cooperation between national energy infrastructure operators and European institutions by contributing operational expertise, regulatory knowledge, and technical insights related to data reporting and transparency mechanisms.
- Developed strong stakeholder management capabilities through continuous collaboration with internal departments, IT teams, regulatory authorities, and European organizations, ensuring alignment between business objectives, technical capabilities, and regulatory obligations.

SNTGN TRANSGAZ S.A.

City: Medias | **Country:** Romania

[09/09/2014 – 30/05/2015] **SCADA Data Analyst | Industrial Systems Analysis**

Key Responsibilities

- Participated in technical working meetings supporting the implementation and optimization of SCADA system projects, contributing to requirements analysis, operational assessments, and alignment between technical solutions and business needs.
- Analyzed functional and technical requirements related to SCADA implementations, evaluating data flows, system capabilities, operational processes, and reporting requirements to support effective deployment and continuous improvement.
- Performed analysis of operational data packages collected by SCADA systems, validating data consistency, identifying trends, detecting anomalies, and providing insights to support operational efficiency and system reliability.
- Processed and interpreted SCADA generated information from industrial monitoring systems, supporting technical teams in evaluating system performance, operational conditions, and infrastructure behavior.
- Developed periodic technical reports, operational analyses, and management information packages for the SCADA Management Unit (U.M.P SCADA) and organizational leadership, transforming technical data into actionable business insights.
- Prepared structured reporting materials for senior management, supporting decision making processes related to operational performance, system improvements, resource planning, and infrastructure reliability.
- Collaborated with engineering, operational, and management teams to ensure accurate communication of SCADA related findings, project progress, risks, and improvement opportunities.
- Supported data driven decision making by improving the visibility, quality, and accessibility of operational information generated by SCADA systems.
- Contributed to documentation activities, including technical analysis reports, operational procedures, and project related information required for effective SCADA system management.

S.C. EMERSON S.R.L

City: Cluj-Napoca | **Country:** Romania

[03/2013 – 29/08/2014] **IT Analyst | Enterprise Applications | Data Analysis & Business Systems Support**

Key Responsibilities

- Provided enterprise IT support and application management services within a global technology environment, ensuring the availability, reliability, and effective use of critical business applications supporting organizational operations.
- Performed analysis, validation, and monitoring of enterprise data stored within SAP and Oracle database environments, ensuring data accuracy, consistency, integrity, and availability for operational and management reporting purposes.

- Managed and supported multiple enterprise applications, including SAP, Oracle, HPSM (HP Service Manager), and ININ, ensuring efficient operation, issue resolution, user support, and alignment with business requirements.
- Provided technical assistance and application support to Emerson employees, troubleshooting incidents, analyzing user reported issues, documenting resolutions, and escalating complex technical problems to specialized support teams.
- Monitored application performance, data flows, and system generated information to identify inconsistencies, operational issues, and opportunities for process improvement.
- Analyzed business data and operational metrics to generate periodic reports, supporting management visibility, decision making processes, and continuous improvement initiatives.
- Prepared structured reports and data analyses by extracting, reviewing, and interpreting information from enterprise systems, transforming technical data into meaningful business insights.
- Participated in internal business and technical meetings, contributing to application reviews, process discussions, requirements analysis, and improvement initiatives.
- Supported the analysis and maintenance of operational matrices, ensuring accurate tracking of performance indicators, service activities, application usage, and business process effectiveness.
- Collaborated with cross functional teams, business users, and technical specialists to improve application reliability, enhance user experience, and ensure effective delivery of IT services.
- Contributed to IT service management processes by supporting incident tracking, issue escalation, documentation, and continuous improvement activities aligned with enterprise support practices.

EDUCATION AND TRAINING

[27/09/2021 – Current]

Phd, National University of Political Studies and Public Administration (SNSPA)

Doctoral Studies on Management http://snspa.ro/en/education/programmes/doctoral-studies/

Address: Exhibition Boulevard, No. 30 A, Sector 1, , Bucharest, Romania

[30/09/2018 – 29/09/2020]

Master's degree - Advanced computer systems and technologies

Faculty of Sciences, Computer Science, Lucian Blaga University http://stiinte.ulbsibiu.ro/info/info/catedra/despre_noi.php

Address: Dr. Ion Ratiu Street, no. 5-7 , 550012 , Sibiu, Romania

[08/06/2024 – 27/09/2024]

Palo Alto Networks Certified Detection and Remediation Analyst PCDRA

PaloAlto https://www.paloaltonetworks.com/

Country: United States | **Field(s) of study:** Information and Communication Technologies: • *Inter-disciplinary programmes and qualifications involving Information and Communication Technologies (ICTs)* | **Level in EQF:** EQF level 8

This certification includes the Palo Alto Networks Cortex XDR: Prevention and Deployment (EDU-260) and Palo Alto Networks Cortex XDR: Investigation and Response (EDU- 262). Recommended Self-paced training include Analyzing and

securing with Cortex XDR and Extending Cortex XDR and Proactive security.

[12/06/2023 – 16/06/2023]

PMP Certification

PM ACCESS https://www.pmaccess.ro/?lang=en

Country: Romania

[12/03/2023 – 27/04/2023]

InsightIDR (Rapid7) Certified Specialist

Rapid7 https://www.rapid7.com/

Country: United States | **Field(s) of study:** Information and Communication Technologies: • *Inter-disciplinary programmes and qualifications involving Information and Communication Technologies (ICTs)* | **Level in EQF:** EQF level 8

[11/04/2022 – 14/04/2022] **Internal auditor ISO/IEC 27001:2013(SR EN ISO 27001:2018) & ISO 19011:2018**

Dekra Srl https://www.dekra.ro/ro/training-planificat-1/

[01/06/2020] **National CTFs competitions**

National Agencies - DNSC

[10/05/2022 – 13/05/2022] **Certified Tester Foundation Level (CTFL) - ISTQB**

ISTQB https://www.istqb.org/

[18/07/2022 – 18/07/2022] **Windows 11 - security by default workshop**

Microsoft https://info.microsoft.com/CE-ZTF-WBNR-FY22-03Mar-30-Windows-11-security-by-default-workshop-SRDEM108118_LP04-Lobby-Page.html

[11/07/2022 – 11/07/2022] **Microsoft Certified: Azure Data Fundamentals**

Microsoft https://docs.microsoft.com/en-gb/certifications/azure-data-fundamentals/?ocid=AID3032310_QSG_529838&mkt_tok=MTU3LUdRRS0zODIAAAGFwPMnunbr9TI0wv5C8GlsKex-wFJd5oU1oJb_Jg85A1GM7p2kSoxyWkuYG4LxW_a8gPpTZOK0QwmouAhGuAFQxz80CYfDaRXuDlPWazb11edWj62YqD566iXX

[27/06/2022 – 28/06/2022] **Microsoft Certified: Security, Compliance, and Identity Fundamentals**

Microsoft https://docs.microsoft.com/en-gb/certifications/security-compliance-and-identity-fundamentals/?ocid=AID3032310_QSG_529861&mkt_tok=MTU3LUdRRS0zODIAAAGF5V7JoNdV8V5ytE43ZSm6XSyPuP2jQF88qjG5H9oYSEcnnJeo5I0wyoYxPrWvQd47YSVslSaq2R7m3S-IuLCeYEEfBSYi1WqWkDOvbIVuf0a-eAkkKu_OTN4I

[30/09/2020 – 29/03/2021] **CCNA Certifications**

Lucian Blaga University, CiSCO Partner https://www.credly.com/earner/earned/badge/01c7ae95-e95a-43ef-89a6-b213f14162da

[31/10/2020 – 31/01/2021] **CompTIA Security+**

[31/01/2014 – 31/03/2014] **CompTIA A+**

CISCO Partner

[01/08/2021 – 11/08/2021] **Course Entry-Level Python Programmer**

Python Institute https://pythoninstitute.org/

[07/06/2021 – 10/06/2021] **Cyber Diplomacy Course | The United Nations Office for Disarmament Affairs**

United Nations https://cyberdiplomacy.disarmamenteducation.org/home/

[31/08/2020 – 29/10/2020] **Linux Fundamentals**

Linux Foundation https://learning.edx.org/

[31/01/2015 – 31/07/2015] **Web Development Programmer**

Swiss WebAcademy

[30/09/2008 – 29/09/2014] **Bachelor's degree, Faculty of Law**

Dimitrie Cantemir University http://www.dimitriecantemir.ro/

Address: Burebista Street, no. 2, 400276, Cluj-Napoca, Romania

[30/09/2005 – 29/09/2008] **Bachelor's degree, Faculty of Economics and Business Administration**

Alexandru Ioan Cuza University https://www.uaic.ro/

Address: Carol I Boulevard, No. 20A, 700505, Iasi, Romania

LANGUAGE SKILLS

Mother tongue(s): Romanian

Other language(s):

English

LISTENING C2 **READING** C2 **WRITING** C1

SPOKEN PRODUCTION C1 **SPOKEN INTERACTION** C1

Italian

LISTENING C2 **READING** C2 **WRITING** C1

SPOKEN PRODUCTION C1 **SPOKEN INTERACTION** C1

French

LISTENING B2 **READING** B1 **WRITING** B1

SPOKEN PRODUCTION B1 **SPOKEN INTERACTION** B1

Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user

SKILLS

Networks: TCP/IP, LAN (Ethernet), Windows Server, Active Directory | Network Security Monitoring | Network and security protocols | Kali Linux (network penetration testing) | BurpSuite | Nmap | WireShark | Snort | NetFlow Tracker | Python | HTML | SQL | CSS | MySQL | Git | JavaScript | Microsoft Office | Linux | Object-Oriented Programming | Bootstrap | JQuery | Web Development | Vulnerability Scanning | Malware analysis - generic approach

CONFERENCES AND SEMINARS

[01/01/2023 – 30/09/2025] **PaloAlto Networks Conferences and Webinars (2023 - 2025)** Online

Starting in 2023, I actively attended multiple conferences, workshops, and webinars with PaloAlto Networks Team on CORTEX XDR, CORTEX Cloud, and XSIAM.

Link: https://www.paloaltonetworks.com/

[23/01/2025 – 24/01/2025] **BSB Lab Symposium 2025** Varese, Italy

Paper: Knowledge Vulnerability. Representation using Tree Diagrams. A Method for Identifying Causes of Knowledge Risks.

https://bslab-symposium.net/Varese-2025/BSLab_Book_of%20_Abstract_T&S_Varese_2025.pdf

Link: https://bslab-symposium.net/Varese-2025/BSLab_Book_of_Abstract_T&S_Varese_2025.pdf

[09/08/2022 – 09/08/2022] **Cortex XSIAM by Palo Alto Networks, Inc.** Virtual

https://www.paloaltonetworks.com/cortex/cortex-xsiam

Link: https://start.paloaltonetworks.com/Cortex-XSIAM

[10/05/2022 – 10/05/2022] **Threat Monitor Webinar** Virtual

Get insights into recent and emerging advances in the threat landscape. Learn how to reduce your exposure to new threats and exploit techniques. Adapt your preventive, detection and response measures to the threat environment.

Link: https://campaign.cybersecurity.nccgroup.com/threatmonitor-webinar

[23/10/2023 – 24/10/2023] **13th edition STRATEGICA** BNR Bucharest

Paper: KNOWN AND UNKNOWN KNOWLEDGE RISKS IN TIMES OF TRANSITION AND CHANGE

https://strategica-conference.ro/wp-content/uploads/2024/10/45.-Vlad-Mihai-URSACHE.pdf

Link: https://strategica-conference.ro/wp-content/uploads/2024/10/45.-Vlad-Mihai-URSACHE.pdf

[26/03/2023 – 28/03/2023] **The 17th International Conference on Business Excellence Rethinking business: Sustainable leadership in a VUCA world** ASE Bucharest

Paper: Knowledge Vulnerabilities Scoring System and the Knowledge Economy

https://www.researchgate.net/publication/369539013_Knowledge_Vulnerabilities_Scoring_System_and_the_Knowledge_Economy

Link: https://bizexcellence.ro/category/icbe-2022/

[20/10/2022 – 21/10/2022] **10th edition STRATEGICA** BNR Bucharest

Paper: Knowledge Risk Management in a Bureaucratic System

https://www.researchgate.net/publication/364772642_KNOWLEDGE_RISKS_MANAGEMENT_IN_A_BUREAUCRATIC_SYSTEM

Link: https://strategica-conference.ro/wp-content/uploads/2022/10/SNSPA-IW-and-STRATEGICA-AGENDA-20.10.2022.pdf

[22/03/2022 – 23/03/2022] **The 16th International Conference on Business Excellence** ASE Bucharest

Presenting my research paper on "Cybersecurity challenges in the knowledge economy". New Challenges of the Century. https://www.researchgate.net/publication/360134378_Cybersecurity_Challenges_in_the_Knowledge_Economy

Link: https://bizexcellence.ro/category/icbe-2022/

[17/03/2022 – 17/03/2022] **CEE Cybersecurity Forum** Virtual

Cybercriminals are targeting and attacking all sectors of critical infrastructure. Ransomware attacks are increasingly successful, crippling governments and businesses, and the profits from these attacks are soaring. The cyberattack landscape becoming increasingly sophisticated as cybercriminals continue their activity in times of crisis.

Link: https://www.crayon.com/campaign/cee-cybersecurity-forum-second-edition/

[16/03/2022 – 16/03/2022] **Nordic Virtual Summit 3. Edition** Virtual

Nordic Virtual Summit is a joint collaboration between the following Scandinavian user groups: MSEndpointMgr.com, MMUGNO, SCUGDK, MMUGSE, SCUGFI.

Link: https://nordicvirtualsummit.com/3rd-edition-agenda/

[14/03/2022 – 14/03/2022] **MANAGING SECURITY RISKS WITH SPLUNK SIEM ENTERPRISE SECURITY - DATANET WEBINAR** Virtual

Link: https://datanets.ro/webinar-gestionare-riscuri-securitate-siem-splunk/

[03/03/2022 – 03/03/2022] **Microsoft Cloud Adoption Framework Webinar Session** Virtual

Link: https://www.crayon.com/ro/channel-partner/resources/partner-events/cloud-adoption-framework-3.03/#msdynttrid=0vwQZPyR2ufbQzIw3DaZJ8RJ8CFojWenaOCKWYnFrzI

[23/02/2022 – 23/02/2022] **Mitigate Risk in the Cloud with Ethical Hackers and DevOps** Virtual | https://www.hackerone.com/events/mitigate-risk-cloud-ethical-hackers-and-devops?ref=infos

Link: https://www.hackerone.com/events/mitigate-risk-cloud-ethical-hackers-and-devops?ref=infosec-conferences.com

[12/10/2021 – 13/10/2021] **The New Global Challenges in Cyber Security" (CERTCON11) organized by The National Cyber Security Directorate (former CERT-RO)** Palace of Parliament & Online

I am still in contact with DNSC and I was involved not only as participant, I was among one of rapporteurs. The report may be provided upon request.

Link: https://dnsc.ro/certcon11/about/#history

[26/09/2021 – 28/09/2021] **GSX x CyberCon Cybersecurity** Online

Debates on cybersecurity challenges.

Link: https://www.cyberconconference.com/

[19/11/2017 – 19/11/2017] **International Conference the European Energy Security** Online

Debates on Regulation on security of gas supply (Regulation (EU) 2017/1938) and the main obligation of Transmission System Operators (OST).

[05/09/2016 – 06/09/2016] **Workshop on Harmonization of Data Exchanges in the European Union** Brussels

Harmonization of Data Exchanges in the European Union

[11/04/2016 – 12/04/2016] **International Conference on Regulation on Wholesale Energy Market Integrity and Transparency (REMIT)** Ljubljana

Regulation on Wholesale Energy Market Integrity and Transparency (REMIT) organized by ACER Agency. Debates on main obligations to report data from contracts and internal systems.

[03/02/2016 – 04/02/2016] **9th Workshop on Transparency Data** Brussels

Workshop on Transparency Data organized by European Network of Transmission System Operators for Gas (ENTSOG). Analysis on REMIT regulation and ENTSOG main obligations to collect data from Transmission System Operators (OST).

Link: https://www.entsog.eu/events/entsog-8th-transparency-workshop

[08/06/2015 – 09/06/2015] **28th session of the Regional Steering Committee of the Regional Initiative for South-Southeast Gas** Bucharest

Regional Steering Committee of the Regional Initiative for South-Southeast Gas, organized by the Romanian Energy Regulatory Authority (ANRE), Hungarian Energy and Public Utility Regulatory (MEKH) and the European Commission.

Link: https://www.acer.europa.eu/gas/network-codes/gas-regional-initiatives/south-south-east-gas-regional-initiatives