القمة الأفريقية للأمن السيبراني
الرباط - المغرب

AFRICAN CYBERSECURITY SUMMIT
RABAT -MOROCCO

African Cybersecurity Summit
Intelligence artificielle et cloud de confiance : Un pilier pour renforcer la cybersécurité
Du 3 au 5 février 2025

Day one – February 3, 2025

08:00 – 08:45 | Badge Collection and Welcome with Refreshments.

08:45 – 08:50 | National Anthem.

08:50 – 09:00 | Opening Speech by the Master of Ceremony.

- Mr. Khalid Al-Amrani.

Official Opening

09:00 – 09:15 | Official Opening Speeches by Ministers.

- H.E. Mr. Abdellatif Loudiyi, Minister Delegate to the Head of Government in charge of National Defense Administration.
- H.E. Ms. Amal El Fallah Seghrouchni, Minister Delegate to the Head of Government in charge of Digital Transition and Administrative Reform.
- Mr. Lacina Koné, Director General and CEO of Smart Africa.

Strategic Vision and Collaboration

09:15 – 09:30 | Keynote 1: Africa's Digital Transformation: Embracing Cybersecurity and Technological Sovereignty.

This keynote introduces the seminar, which will focus on the crucial role of robust, sovereign cybersecurity in enabling resilient digital transformation across Africa. Through examples, it highlights how innovative technologies can safeguard critical infrastructures and strengthen the continent's digital ecosystem. It also emphasizes the importance of initiatives like Smart Africa and the African Network of Cybersecurity Authorities (ANCA) in harmonizing digital policies among African nations and fostering capacity building through a collaborative and visionary approach.

- Mr. Brigadier General El Mostafa Rabii, Vice President of the ANCA Cybersecurity Authority Alliance.

09:30 – 10:10 | Panel 1: Strengthening Africa's Digital Resilience: AI, Trusted Cloud, and Federated Cloud as Strategic Catalysts.

This panel will explore practical approaches to enhancing Africa's digital resilience by harnessing the potential of artificial intelligence (AI), Trusted Cloud, and federated cloud solutions.

Drawing on both international and African experiences, the discussion will examine into operational strategies, the development of sustainable ecosystems, and the essential public-private collaborations needed to build a secure and sovereign digital future. By presenting concrete examples, the panel aims to translate strategic discussions into actionable steps tailored to Africa's unique contexts.

- H.E. Shaikh Salman bin Mohammed Al-Khalifa, CEO National Cyber Security Centre (NCSC), Bahrain.
- Dr. Ammar Hassan Al-Husseini, Former Director General, Central Agency for Information Technology (CAIT), Kuwait
- Executive Committee Member, Google Agreement for Technology Development, Kuwait.
- Dr. Albert Antwi-Boasiako, Director-General of Ghana's Cyber Security Authority (CSA) and President of the ANCA Cybersecurity Authority Alliance.
- Mr. Bassam Maharmeh, President of the National Cyber Security Center (NCSC), Jordan.
- Mr. Khalil Nossair, Director of Assistance, Audit, Training, Control and Expertise, DGSSI.
- Dr. Redda Ben Geloune, Artificial intelligence expert with extensive experience in Africa, focusing on AI for economic and technological development.
- Ms. Neama Benhammou, Cybersecurity Manager.

10:10 – 10:25 | Keynote 2: Bridging Continents: Strengthening Cybersecurity Through Collaborative Capacity Building and Shared Expertise.

This keynote will focus on the need to establish a pan-African entity operationally affiliated with ANCA, inspired by the model of the ITU's Arab Regional Cybersecurity Center (ARCC). Such a structure would play a strategic role in enabling real-time threat intelligence sharing, coordinating incident responses, and enhancing resilience against cross-border cyber threats. It will also explore ways to strengthen cooperation between ANCA and the National Cybersecurity Centers of the Organization of Islamic Cooperation (OIC) member states. This mutually beneficial collaboration would facilitate the exchange of experiences and best practices while supporting the implementation of training programs and regional exercises to enhance the cybersecurity capabilities of both parties.

- Engineer Badr Ali Al-Salehi, Director General, Oman National CERT, Chairman of OIC National Cybersecurity Centers Head of ITU Regional Cybersecurity Center, Oman.

10:25 – 10:35 | Keynote 3: The Evolution of AI and Trusted Cloud: Shaping the Future of Industrial Resilience.

This keynote will explore how artificial intelligence (AI) and trusted cloud technologies are transforming critical infrastructures by fostering innovation, enhancing resilience, and enabling secure digital transformation. It will delve into advancements in AI and cloud infrastructure, highlighting their wide-ranging applications across sectors such as healthcare, transportation, and energy.
The session will emphasize the strategic benefits of these technologies in tackling industry-specific challenges, promoting sustainability, and optimizing operational efficiency.

- Mr. Sean Yang, Director of the Global Cybersecurity and Privacy Protection Office. Huawei Group.

القمة الأفريقية للأمن السيبراني
الرباط - المغرب

AFRICAN CYBERSECURITY SUMMIT
RABAT -MOROCCO

Securing Critical Sectors and Industrial Operations

10:35 – 11:05 | Panel 2: Enhancing the Security and Efficiency of Industrial Operations in the Era of AI and Cloud: Focus on the Oil and Gas Sector.

This panel will examine the strategic impact of qualified cloud computing and artificial intelligence (AI) on securing and optimizing industrial operations, particularly within the oil and gas industry. It will provide strategic and operational insights to professionals in the petroleum, gas, and industrial sectors, offering concrete solutions for effectively integrating AI and qualified cloud services into their digital transformation processes.

- Mr. Khalfan bin Salem bin Juma Al-Kaabi, Director of Cybersecurity Solutions at OQ Group, Oman.
- Mr. Mohamed Hassan, Chief Operating Officer (COO), Muscat Investment House (MIH), Oman.
- Ms. Denyse Ntaganda, Associate Project Manager, Digital Access and Connectivity, Smart Africa.
- Engineer Badr Ali Al-Salehi, Director General, Oman National CERT, Chairman of OIC National Cybersecurity Centers Head of ITU Regional Cybersecurity Center, Oman.
- Mr. Amine Kandil, founder and CEO of OneCloud.
- Ms. Neama Benhammou, Cybersecurity Manager.

11:05 – 11:20 | Keynote 4: Proactive Risk Management for Securing Critical Sectors.

This keynote will provide an in-depth look at how artificial intelligence is deployed to secure critical sectors such as energy, healthcare, and finance. Through real-world case studies, the presentation will demonstrate AI's powerful capabilities in detecting and preventing cyber threats before they cause harm. By focusing on proactive risk management, AI enhances the security posture of these essential infrastructures, reduces operational vulnerabilities, and minimizes downtime caused by cyber incidents. Attendees will gain practical insights into how AI solutions are being integrated into cybersecurity strategies to strengthen resilience and maintain the continuity of critical services.

- Ms. Kirsty Paine, Field CTO, Cisco.

11:20 – 11:55 | Panel 3: Cybersecurity Strategies for Major International Events: Lessons from the FIFA World Cup.

This panel examines the unique cybersecurity demands of hosting large-scale international events, such as the FIFA World Cup. Experts will discuss frameworks for securing critical infrastructure, managing real-time threats, and ensuring compliance with cybersecurity standards. Panelists will also explore the role of (AI) in threat monitoring and incident response, as well as the importance of international cooperation among security teams.

- Mr. Bashar Ismail Amin Al Khatib, V-CISO - FIFA WORLD CUP Qatar 2022, FIFA.
- Mr. Sami Mohammed Hussein Al-Shammari, Leader in Infrastructure and Operations for the FIFA World Cup 2022, Qatar.
- Mr. Assad Arabi, Managing Director of Gulf and Emerging Markets, Trend Micro.
- Ms. Hind El Fal, Executive Director, Orange.
- Ms. Nor El Houda Sabbar, Cybersecurity Ecosystem Director, Dataprotect.
- Ms. Neama Benhammou, Cybersecurity Manager.

11:55 – 12:10 | Keynote 5: Enhancing Critical Infrastructure Resilience Against Cyber Threats.

This keynote will delve into the application of artificial intelligence to strengthen the resilience of critical infrastructure against cyber threats. AI technologies, such as real-time monitoring and threat-neutralization capabilities, are pivotal in securing essential sectors like energy, transportation, and healthcare. By leveraging AI, these sectors can detect vulnerabilities and respond to threats proactively, ensuring continuous operation and reducing downtime. Through practical examples, the presentation will demonstrate AI's role in predicting potential risks, streamlining incident responses, and providing robust defenses to maintain the stability and security of essential services.

- Mr. Ali El Azzouzi, Founder and CEO, Dataprotect.

12:10 – 12:30 | Coffee Break.

Data Ethics, Protection, and Development

12:30 – 12:45 | Keynote 6: Securing Trusted Cloud Environments: Data Protection and Threat Detection.

This session will explore how artificial intelligence is leveraged to secure Trusted Cloud environments, focusing on three critical areas: safeguarding sensitive data, detecting sophisticated threats, and ensuring compliance with digital sovereignty standards. As governments and organizations increasingly adopt Trusted Clouds to maintain control over data within national borders, the role of AI becomes vital. The presentation will highlight AI-driven solutions that provide enhanced data protection, real-time threat identification, and adherence to regulatory and sovereignty requirements.

- Dr. Bilal Issa, Technical & Support Manager, Trend Micro.
- M. Gopaul Jotish Ashvin, Trend Micro.

12:45 – 13:00 | Keynote 7: The Evolution of AI and Cloud: Shaping the Future of Digital Resilience.

The session will focus on the strategic advantages of these technologies in addressing industry-specific challenges, promoting sustainability, and optimizing operational efficiency.

- Ms. Li Hualan, Cybersecurity Expert, HQ Huawei Group.

13:00 – 13:30 | Panel 4: Navigating AI in Cybersecurity: Development and Ethics.

This panel will delve into the multifaceted role of artificial intelligence (AI) in cybersecurity, focusing on secure development practices, ethical considerations, and enhancing infrastructure resilience. Experts will discuss challenges and strategies in developing secure AI systems, address ethical dilemmas such as privacy and accountability, and explore how robust infrastructures can bolster cybersecurity measures. The session aims to provide a comprehensive understanding of AI's impact on cybersecurity and offer actionable insights for practitioners and policymakers.

- Mr. Olivier Gakwaya, Project Manager for Emerging Technologies, Smart Africa.
- Mr. Ait Kaddour Youssef, Cybersecurity and Privacy Protection Director, Huawei Maroc.
- CBI, to be determined (TBD).
- Techso Group - IBM, to be determined (TBD).
- Mr. Reda El Bakkali, CEO Groupe INEOS-CYBERFORCES, Cyberforces.
- Moderator: Ms. Yenataba Kignaman-Soro: Senior Cybersecurity Consultant.

Innovations in Compliance and Secure Development

13:30– 13:45 | Keynote 8: Transforming Secure Software Development: Proactive Threat Management and Automation.

This presentation will delve into the transformative role of artificial intelligence in enhancing secure software development. The session will highlight AI-driven solutions that support proactive threat anticipation, automate essential security controls, and bolster overall software reliability. By integrating AI into development workflows, organizations can streamline security checks, identify vulnerabilities early, and ensure continuous protection throughout the development lifecycle. Speakers will share practical insights and real-world examples, illustrating how AI can be embedded into development processes to build more resilient, secure, and robust software solutions.

- Ms. Nouhade Machkour, Directeur Solutions Techniques B2B, Orange.

13:45 – 14:00 | Keynote 9: Streamlining Cybersecurity Compliance and Risk Management.

This session will explore how AI can assist organizations in adhering to increasingly stringent cybersecurity regulations. Through advanced analysis and automation techniques, AI enables real-time monitoring of security practices, detection of compliance violations, and risk anticipation. Participants will learn how AI tools can simplify compliance management and strengthen organizational resilience against cyber threats while meeting international standards and legal requirements.

- Mr. Alain Sanchez, Field CISO, Fortinet

14:00 – 15:00 | Lunch Break.

15:00 – 18:00 | ANCA Meeting.

19:00 – 21:00 | Dinner.

القمة الأفريقية للأمن السيبراني
الرباط - المغرب

AFRICAN CYBERSECURITY SUMMIT
RABAT -MOROCCO

Day Two – February 4, 2025

08:50 – 09:00 | Opening Speech by the Master of Ceremony.

- Mr. Khalid Al-Amrani.

Official Opening

09:00 – 09:15 |Opening Keynote: Securing Africa's Digital Future: Strengthening Sovereignty and Resilience.

This keynote offers a forward-looking perspective on leveraging artificial intelligence (AI) to secure Africa's digital landscape. It will delve into how AI can strengthen digital sovereignty, safeguard Africa's unique digital assets, and establish an ethical framework for its application in cybersecurity. Attendees will gain valuable insights into the opportunities and challenges of AI adoption, with concrete examples of how AI can enhance Africa's digital resilience and bolster cybersecurity efforts across the continent.

- Dr. Redda Ben Geloune: Artificial intelligence expert with extensive experience in Africa, focusing on AI for economic and technological development.

09:15 – 09:30 |Opening Keynote: Vision of ANCA's Priorities and Actions to Ensure a Secure and Sustainable African Cyberspace.

In this keynote, the President of the African National Cybersecurity Authorities Alliance (ANCA) will present the main decisions taken during the latest annual meeting, highlighting the progress made. He will also outline ANCA's strategic action plan for the coming years, focusing on strengthening regional cooperation, harmonizing cybersecurity legislation, and implementing concrete initiatives to build a more resilient Africa in the face of cyberattacks.

- Dr. Albert Antwi-Boasiako, Director-General of Ghana's Cyber Security Authority (CSA) and President of the ANCA Cybersecurity Authority Alliance.

Empowering Africa's Cybersecurity through AI Innovation and Collaboration

09:30 – 10:15 | Panel 1: Forging a Unified Path: AI Governance and Cybersecurity in Africa.

This session will convene prospective members of the AI Governance Council and representatives from the African Network of Cybersecurity Authorities (ANCA) to collaboratively develop a comprehensive roadmap for AI governance and cybersecurity across the continent. Participants will identify synergies between AI initiatives and cybersecurity frameworks, aiming to establish cohesive strategies that address Africa's unique challenges and opportunities in the digital landscape. The discussion will focus on aligning objectives, setting actionable goals, and fostering partnerships to enhance digital resilience and ethical AI deployment throughout Africa.

- Mr. Saad El Khadiri, Director of Strategy and Regulation, DGSSI.
- Mr. Bassirou Abdoul Ba, Director General of Senegal Connect Park.

- Mr. Olivier Gakwaya, Project Manager for Emerging Technologies, Smart Africa or Ms. Denyse Ntaganda: Associate Project Manager, Digital Access and Connectivity, Smart Africa.
- Mr. Ait Kaddour Youssef, Cybersecurity and Privacy Protection Director, Huawei Maroc.
- Dr. Bilal Issa, Technical & Support Manager, Trend Micro.
- Moderator: Ms. Yenataba Kignaman-Soro: Senior Cybersecurity Consultant.

10:15 – 10:30 | Keynote 1: Building Resilient Digital Infrastructures: Africa's Path to Cybersecurity Excellence.

This keynote addresses Africa's pivotal role in the global digital economy, emphasizing the critical need for robust cybersecurity measures and technological sovereignty to ensure sustainable development. It explores the integration of innovative technologies such as artificial intelligence and Trusted Cloud solutions to protect critical infrastructures and drive economic growth. The importance of harmonizing digital policies across African nations is underscored, fostering collaboration through initiatives like Smart Africa and the African Network of Cybersecurity Authorities (ANCA). Developing local capacities is highlighted as essential to achieving a secure and prosperous digital future for the continent.

- Mr. stephane Guelfo, SVP Business Solutions, OneCloud.

10:30 – 10:45 | Fireside Chat: Launch of Dr. Albert Antwi-Boasiako Book.

This fireside chat marks the launch of a pivotal work in cybersecurity focused on Africa. Dr. Albert Antwi-Boasiako's book delves into innovative strategies for enhancing digital resilience and addressing evolving cyber threats. It offers practical solutions to critical challenges both in Africa and on a global scale.

- Dr. Albert Antwi-Boasiako, Director-General of Ghana's Cyber Security Authority (CSA) and President of the ANCA Cybersecurity Authority Alliance.
- Ms. Neama Benhammou, Cybersecurity Manager.

10:45 – 11:15 | Panel 2: Building a Cybersecurity Workforce for the Future.

This panel will explore strategies for developing skilled cybersecurity professionals to address evolving threats. Discussions will include capacity building, fostering public-private partnerships, promoting diversity in cybersecurity, and ensuring continuous learning through educational and training initiatives.

- Dr. Assane Gueye Professor, Carnegie Mellon University Africa Co-Director, Upanzi Network and CyLab-Africa Initiatives Guest Researcher, National Institute of Standards and Technology (NIST), USA.
- Mr. Yasir El Kabbany, Senior Regional Director, Middle East & Africa, CompTIA.
- Ms. Kirsty Paine, Field CTO, Cisco.
- Techso Group - IBM, to be determined (TBD).
- Mr. Mohamed Sekkat, CBO, Casanet.
- CBI, to be determined (TBD).
- Ms. Neama Benhammou, Cybersecurity Manager.

11:15 – 11:45 | Panel 3: Emerging Cybersecurity Trends in Africa: Navigating the Evolving Threat Landscape.

This session will explore the latest developments in cyber threats across the continent, including the rise of ransomware, phishing schemes, and data breaches. Experts will discuss the implications of these trends and share best practices for organizations to strengthen their cybersecurity posture in response to the evolving threat environment.

- Logrythm/exabeam, to be determined (TBD).
- Mr. Dominique Meurisse, VP International, Gatewatcher.
- Mr. Keyser Tabi, SOC Manager, Dataprotect.
- Mr. Waseem Youssef, Sr Director Technical Solutions & Systems Engineering NW Africa, Palo Alto Networks.
- BeyondTrust - Sophos, to be determined (TBD).
- Orange Cyberdefense, to be determined (TBD)
- Moderator: Ms. Yenataba Kignaman-Soro: Senior Cybersecurity Consultant.

11:45 – 12:00 | Coffee Break.

12:30 – 14:30 | Sessions 1, 2, 3, 4, 5 and 6 (in parallel).

Session 1: Predictive Threat Analysis with AI and Metadata

Real-Time Threat Detection:

Explore how AI improves the preemptive identification of emerging threats by leveraging metadata standards like CVE and CVSS. (Focuses on early detection to prevent escalation, distinct from incident handling.)

Predictive Risk Management with EPSS and VEX:

Use tools like EPSS and VEX to forecast potential attack vectors and prioritize vulnerabilities for proactive defenses. (Focuses on forecasting and prioritization, separate from long-term management workflows.)

- Logrythm/exabeam, to be determined (TBD).

Session 2: AI-Driven Threat Intelligence and Strategic Security Planning in DevSecOps

Harnessing Threat Intelligence with AI.

This session will focus on how organizations can leverage AI to gather, analyze, and act on threat intelligence. Participants will explore techniques to integrate AI into DevSecOps workflows for real-time threat detection, prioritization of risks, and rapid decision-making based on global threat feeds and emerging attack patterns.

Proactive Risk Mitigation Through Strategic Insights.

Participants will learn how AI can provide strategic insights by correlating data from diverse sources, enabling informed security planning. This section will focus on creating adaptive risk management frameworks that dynamically adjust to the evolving threat landscape.

Scenario-Based Security Simulation and Planning.

The final part of the session will include practical exercises in AI-powered scenario simulation. Participants will learn to forecast potential attack vectors, evaluate their security posture, and design robust incident response plans based on predictive threat modeling and historical data analysis.

- Mr. Imad Abdessadki, Directeur de la BU Offensive Security, Dataprotect.

Session 3: Securing Infrastructure and Data

Critical Infrastructure Resilience:

Examine long-term strategies using AI to dynamically protect critical systems against evolving threats. (Focuses on adaptive security strategies for essential systems.)

Cloud Data Security:

Learn how AI secures cloud environments by monitoring data flows and detecting breaches specific to cloud vulnerabilities. (Dedicated to cloud-specific challenges, distinct from general automation.)

IoT Device Protection:

Explore AI-driven solutions for protecting IoT networks by identifying vulnerabilities and mitigating device-targeted threats. (Specialized in IoT security, avoiding overlap with broader infrastructure topics.)

AI for Identity and Access Management:

See how AI enhances IAM systems through anomaly detection and automated security controls. (Targets IAM-specific improvements, separate from general infrastructure or automation discussions.)

- Huawei, to be determined (TBD).

Session 4: Strategic Vulnerability Management

Streamlined Vulnerability Management with AI:

Use AI to enhance workflows for identifying, prioritizing, and remediating vulnerabilities, improving overall security posture. (Focuses on strategic planning, avoiding overlap with real-time operational processes.)

Standards-Driven Management Frameworks:

Discover how to integrate metadata standards like CVE, CVSS, EPSS, and VEX into long-term vulnerability management strategies. (Emphasizes strategic integration, separate from forecasting tools in Session 1.)

Proactive Vulnerability Optimization:

Learn advanced techniques to transform vulnerability management processes, reducing risks and boosting efficiency. (Dedicated to workflow transformation, avoiding overlap with operational task automation.)

- Mr. Bilal Issa, Technical & Support Manager, Trend Micro.

Session 5: Mastering Security with AI

Unlocking AI's Potential for Cyber Defense

Dive into the transformative power of Machine Learning (ML) and Artificial Intelligence (AI) in enhancing security operations. Discover how these technologies can detect threats, uncover suspicious activities, and strengthen your defenses.

Hands-On Learning with Real-World Scenarios

Engage in practical exercises that replicate real-world challenges, equipping you with the skills to apply ML and AI effectively in security workflows.

Seamless Integration for Advanced Threat Detection

Learn how to integrate ML and AI into your existing processes to optimize threat detection and improve response times, staying ahead in an evolving cybersecurity landscape.

- Cisco, to be determined (TBD).

Session 6: Enhancing Cloud Security with AI: Challenges and Solutions

Securing the Cloud with AI

This session will explore how Artificial Intelligence (AI) is being leveraged to enhance cybersecurity in cloud environments. Participants will learn about AI-driven tools that provide real-time threat detection, anomaly identification, and automated responses to mitigate risks associated with cloud infrastructure.

Challenges and Solutions in Cloud Security

We will discuss the unique cybersecurity challenges that arise in cloud environments, such as data privacy concerns, multi-cloud configurations, and securing cloud-native applications. Experts will share best practices and AI-powered solutions to address these challenges effectively.

Practical Approaches for AI Integration

Through real-world case studies, this workshop will guide participants on how to seamlessly integrate AI into their cloud security strategies. Attendees will gain hands-on experience in applying AI to enhance threat intelligence, improve compliance monitoring, and automate security operations in the cloud.

- OneCloud, to be determined (TBD).

14:30 – 15:30 | Lunch Break.

19:00 – 21:00 | Gala Dinner.

القمة الأفريقية للأمن السيبراني
الرباط - المغرب

AFRICAN CYBERSECURITY SUMMIT
RABAT -MOROCCO

Day Three – February 5, 2025

09:00 – 11:30 | Sessions 7, 8, 9, 10, 11 and 12 (in parallel).

Session 7: Incident Analysis and Rapid Response

Forensic Analysis with AI.

This workshop will address using AI in post-incident analysis to accelerate cybercriminal investigations by automating the collection and analysis of digital evidence.

AI Integration in Security Operations Centers (SOC).

The integration of AI in SOCs will be explored to improve real-time incident management, automating continuous monitoring and response to threats.

AI and Cyberattack Simulation for System Resilience Testing.

This workshop will show how AI can be used to simulate complex cyberattacks, enabling resilience testing and strengthening defenses against real threats.

- CBI, to be determined (TBD).

Session 8: Threat Prevention and Identification

Advanced Phishing Detection with AI.

Participants will learn to use AI to detect phishing attempts and other cyberattacks by analyzing suspicious behaviors and identifying real-time threats.

Integrating AI in Intrusion Detection Systems (IDS).

This workshop will demonstrate how to integrate AI in IDS to enhance real-time threat detection by analyzing abnormal behaviors and automating responses.

Predictive Cybersecurity with AI: Anticipating Threats.

The focus will be on using AI to anticipate cyber threats before they appear by analyzing large-scale data and identifying potential attack patterns.

Using AI for Online Fraud Prevention.

This workshop will focus on detecting and preventing online fraud using AI by analyzing suspicious behaviors and identifying abnormal transactions.

- Techso Group - IBM, to be determined (TBD).

Session 9: Advanced Threat and Attack Prediction

Advanced Threat Analysis and Attack Prediction.

This workshop will explore using machine learning and deep learning to analyze large datasets and identify potential threats before they occur.

Internal Threat Detection Using AI.

Participants will learn to use AI to detect internal threats and analyze abnormal behaviors to identify suspicious activities from employees or compromised devices.

- Philippe Gillet, CTO, Gatewatcher.

Session 10: AI-Driven Strategies for Cyber Defense

Proactive Threat Intelligence

Harness the power of machine learning to revolutionize cybersecurity strategies. This segment will focus on how advanced algorithms enable the early detection of complex threats, providing organizations with the tools to anticipate and mitigate risks before they escalate.

AI-Powered Behavioral Analytics

Dive into the application of AI-driven behavioral analysis to identify subtle anomalies in user and device activities. Learn how these insights can uncover insider threats, unauthorized access attempts, and compromised systems, strengthening overall security.

Transforming Cyber Defense with AI

Explore the broader impact of artificial intelligence on modern cyber defense. From predicting attacks to enhancing decision-making processes, this session will showcase how AI is reshaping the landscape of proactive cybersecurity.

- BeyondTrust - Sophos, to be determined (TBD).

Session 11: Data Security and Regulatory Compliance

Securing Generative AI.

This workshop will address protecting generative AI models, explaining how to secure the data they handle and prevent misuse.

Developing AI Algorithms for Personal Data Protection.

Participants will discover how AI can be used to strengthen personal data protection while ensuring compliance with privacy regulations.

AI for Cybersecurity Regulatory Compliance.

This workshop will demonstrate how AI can help organizations automate cybersecurity audits and ensure compliance with security standards.

- Mr. Alain Sanchez, Field CISO, Fortinet.

Session 12: Enhancing Risk Management in DevSecOps for Secure Development

Security Automation with AI in DevSecOps.

This session will focus on how AI can automate and strengthen security processes in DevSecOps. Participants will discover how AI can be integrated into development tools to analyze code in real-time, identify vulnerabilities early in the development cycle, optimize security tests in CI/CD pipelines, and expedite issue resolution.

Continuous Monitoring for Security in Development Environments.

The second part will address continuous monitoring of development and production environments. AI enables proactive analysis of suspicious activities and abnormal behaviors, ensuring that vulnerabilities and potential threats are detected and addressed quickly.

Risk Reduction and Incident Response Optimization.

This final part will focus on how AI optimizes responses to security incidents, minimizing the impact of attacks. Coupled with DevSecOps practices, AI enables proactive incident management through vulnerability prioritization, quick response automation, and reduced intervention times.

- Mr. Amjad Jabali, Solutions Consultant Prisma Cloud, Palo Alto Networks.

11:30 – 12:00 | Coffee Break.

12:00 – 12:30 | Interactive Business-to-Business (B2B) Session.