DIGITOPIA

FIRST EDITION - Summer 2025

CYBERSECURITY CHALLENGES

Ministry of Communications and Information Technology

www.digitopia.gov.eg

Ministry of Communications and Information Technology

DIGITOPIA

Category	Challenge	Challenge Title	Problem Statement
Elementary Education – Grades 4 to 6 (مستكشف الأثر)	Secure Your Health Data	Patient Data Lock Box	Create a digital "locker" app that stores mock patient data with password protection.
		Cyber Hygiene Game for Physicians	Design a game that teaches medical staff best cyber practices.
	Secure UI	Strong Password Generator and Password Strength Analyzer	Build an app that can help users to generate strong passwords and can evaluate a password for strength improvements.
		Cyber Safe ATM Interface	Simulate a secure ATM interface with PIN entry, keypad masking, and alerts for wrong PINs.
		Phishing Email Spotter Game	An interactive game used to differentiate between fake and real emails.
	Secure Your Online Government Services	Government Service Login App	Build a citizen login app for governmental services using simple authentication techniques such as passwords, OTPs, etc..
		Secure E-Voting System	Create a secure voting app that logs each vote and allows auditing.
	Cybersecurity Aware Generation	Digital Safety Bots or Games	Design an educational mobile game or a chatbot that teaches secure online behavior and shares daily digital safety tips
		Online Harassment & Bullying Protector	Create an anonymous reporting and support platform focused on protecting vulnerable groups, including features to address child exploitation and online harassment, offering resources, counseling referrals, and tools to safely report abuse.

Ministry of Communications and Information Technology

DIGITOPIA

Category	Challenge	Challenge Title	Problem Statement
Preparatory and Secondary Stage (صانع الأثر)	Secure Your Health Data	Encryption App for Medical Records	Create a visual tool showing how encryption protects health data.
		Ransomware Simulator for Hospitals	Simulate a ransomware attack that encrypts files and illustrates the recommended response steps.
	Secure UI	Multi-Factor Authentication Login System	Create a login system with password + mock OTP or biometric scan.
		QR Code Scanner with Fraud Filter	An app that illustrates the scanning and verification of QR payment codes in addition to filtering fake codes.
		Biometric Spoofing Test App	Explore how biometric authentication can be fooled using fake data.
	Secure Your Online Government Services	Secure Citizen Data Vault using Blockchain Technology	Build a simple blockchain simulation for securely storing citizen data.

Ministry of Communications and Information Technology

DIGITOPIA

Category	Challenge Sector/Use Case	Challenge Title	Problem Statement
Preparatory and Secondary Stage (صانع الأثر)	Safety Online Shield	Digital Footprint Detective	Use your programming skills to create a fun and interactive game or quiz that helps players decide what information is safe to share online and what should be kept private.
		Cyber Threat Alarm	Make a fun project that warns you if you do something unsafe on a computer. For example: you can pretend to do something risky (like using an easy password or clicking a fake link).An alarm sound or a warning message that pops up. A message that simply explains why what you did isn't safe.
		Virus Detector	Make a fun game where you destroy different types of computer viruses! Viruses look like funny, moving bugs on the screen. You can use a "cyber shield" or "laser" to blast and stop them. Try to get the highest score and see your name on the leaderboard!
		Play safely	make a platform that teaches others how to play games safely online! Show tips like not sharing real names, using strong passwords, and telling an adult if something feels wrong. Make it fun and easy to understand!
		Arabic Phishing Simulator	Build a simple quiz or app that trains users to spot phishing or scam messages (SMS, email, or social media posts)., specifically using examples and scenarios in Egyptian Arabic to make the training more relatable and effective for local users.
		Media Literacy Game	Design an interactive app or game that educates users—especially youth—on how to recognize fake news, bots, and propaganda techniques especially on social media websites.
		Parental Guidance App	Develop an app that helps parents monitor and educate their children on safe internet use by tracking visited websites (e.g., alerting if pornographic or inappropriate sites are accessed) and monitoring time spent on gaming or other types of websites to promote healthy digital habits.

Ministry of Communications and Information Technology

DIGITOPIA

Category	Challenge	Challenge Title	Problem Statement
Undergraduate Students (مبتكر الأثر)	Cyber Explorers: Learning to Outsmart Online Threats	Threat Intelligence Platform	Develop a Threat Intelligence Platform (TIP) that aggregates, analyzes, and visualizes real-time cyber threat data from multiple sources (e.g., open-source feeds, dark web, internal logs). The platform should enable security teams to quickly identify emerging threats relevant to the organization, enrich alerts with contextual information, and automate recommendations for response actions. Ensure the solution demonstrates measurable business value by reducing incident response time and improving threat detection coverage.
	Silent Vigilant: Digital Tools for a Safer Society	Anonymous Crime Reporting	Build a secure platform that allows citizens to report crimes or misconduct anonymously while protecting their identity using encryption or decentralized networks.
		Emergency Response Map	Develop a real-time, community-driven platform that maps urgent incidents (e.g., fires, car accidents, collapsing building…etc.) and connects them with emergency services
		Victim Support and Legal Aid Chatbot	Design a chatbot that provides confidential guidance on legal rights, how to file complaints, and where to find support for victims of crime or abuse.
	Track & Trust: Tech Solutions to Fight Black Market & Counterfeit Trade	Product Verification App	Build a mobile app for verifying medicine authenticity using QR codes or serial numbers.

Ministry of Communications and Information Technology

DIGITOPIA

Category	Challenge	Challenge Title	Problem Statement
Undergraduate Students (مبتكر الأثر)	Track & Trust: Tech Solutions to Fight Black Market & Counterfeit Trade	Product Verification App	Build a mobile app for verifying medicine authenticity using QR codes or serial numbers.
		Whistleblower Platform	Create a secure tool for citizens or workers to report black market activity anonymously.
		Smart Supply Chain Tracker	Develop a dashboard for tracking goods movement from source to point-of-sale using blockchain or IoT.
		Food Safety Alert System	Design a system that flags unsafe or unlicensed food products based on user reports and inspections.
	TruthHack: Defending Reality in the Age of Deep fakes & Misinformation	Deep fake Detector	Build an AI-powered tool that identifies manipulated videos, images or audio, flagging potential deep fakes in real time.
		FactCheck Plug-in	Create a browser extension or chatbot that verifies the credibility of news articles or social media posts, using trusted databases and NLP.
		Disinformation Campaign and Source Attribution Tracker	Develop a dashboard that visualizes the spread of viral misinformation, identifying sources, amplification patterns, and targeted audiences. For example: An app that flags coordinated inauthentic behavior or state-sponsored influence by tracing patterns in news copy-paste behavior and translation artifacts.
		Narrative Manipulation Pattern Miner	Build a tool that analyzes evolving misinformation narratives by tracking linguistic framing, emotional tone, and timing strategies over time. Unlike origin tracking, this focuses on how coordinated campaigns shift public opinion or distort facts through repetition, sentiment engineering, and selective emphasis. Example: A timeline-based system that surfaces recurring rhetorical tactics or language shifts across campaigns.

Ministry of Communications and Information Technology

DIGITOPIA

Category	Challenge	Challenge Title	Problem Statement
Graduates up to 35 years old (قائد الأثر)	Resilience & Trust: Advanced Security Innovations	Business Continuity & Disaster Recovery Tools	Create planning or simulation tools to help public services prepare for cyber-disruptions. For instance, simulate a ransomware attack on a municipality and design a response tool with playbooks and fallback protocols.
		GRC Systems for Financial Sector	Build governance, risk, and compliance tools tailored to banking and financial institutions. Example: A dashboard that integrates real-time threat monitoring with policy enforcement for internal auditors.
		Digital Twin Systems for Cybersecurity	Design a digital twin model to simulate and enhance security for critical infrastructure, such as simulating attacks on a smart grid to test defense mechanisms and real-time monitoring protocols.
		Hardware and Firmware Security Analysis	Analyze or secure embedded systems and IoT firmware, including BIOS/UEFI or microcontroller-based devices. For example: Extract firmware from a smart device and find hidden backdoors or write a secure bootloader to prevent tampering.
		Static/Dynamic Malware Analysis for Smartphones	Design a toolkit or service for analyzing suspicious mobile apps using static code inspection and dynamic behavior monitoring. Example: Create a sandbox environment that logs system calls and network activity of Android apps to detect malicious patterns.
		Next-Generation Firewall Systems	Design or enhance intelligent firewall architectures capable of detecting sophisticated attacks, encrypted threats, and anomalous behavior using AI and real-time threat intelligence. Example: Build a firewall prototype with L7 inspection and ML-powered anomaly detection tailored for SMB or critical infrastructure environments.

Ministry of Communications and Information Technology

DIGITOPIA

Category	Challenge	Challenge Title	Problem Statement
Graduates up to 35 years old (قائد الأثر)	Resilience & Trust: Advanced Security Innovations	Red vs Blue Simulated Attack-Defense Environments	Build a virtualized environment where teams can take on offensive (Red Team) or defensive (Blue Team) roles to simulate real-world cyberattacks and defense strategies. For example: Create a CTF-like environment with vulnerable servers, where defenders must detect, respond, and patch breaches while attackers try to escalate privileges.
		Data Privacy in the Age of AGI & LLMs	Propose privacy-preserving mechanisms or audit tools to protect user data in AI-driven environments. This could include building a consent-aware data access system or testing a differential privacy wrapper for LLM interactions.
		Smart City Security Frameworks	Design a security management dashboard or alerting system for smart city components (e.g., traffic lights, utilities, CCTV). Example: Build an IoT threat detection engine for a municipal network.
		Secure ITS (Intelligent Transportation Systems)	Propose cybersecurity measures for intelligent transportation platforms such as vehicle-to-infrastructure (V2I) networks or automated tolling. Example: Build a proof-of-concept intrusion detection system for V2X communication nodes.
		Fully Homomorphic Encryption (FHE) Authentication Framework	Develop an authentication system based on fully homomorphic encryption to perform identity verification or access control checks without decrypting sensitive user data. Example: A cloud-based login system that can authenticate users while maintaining complete encryption of their credentials throughout the process.
		Post-Quantum Cryptography Protocols	Develop or test encryption schemes resilient to quantum computing threats. For example, implement a hybrid encryption model using lattice-based algorithms integrated with current public key infrastructure.

Ministry of Communications and Information Technology

DIGITOPIA

Category	Challenge	Challenge Title	Problem Statement
Graduates up to 35 years old (قائد الأثر)	Resilience & Trust: Advanced Security Innovations	Countering Reverse Engineering in Software & AI Models	Create protective layers or obfuscation techniques to make it more difficult for adversaries to reverse-engineer compiled software or machine learning models. Example: Build a prototype that adds anti-debugging and code obfuscation to a sensitive Python-based AI application
		Secure Identity in Blockchain & Decentralized Environments	Develop a privacy-preserving identity management system using decentralized identifiers (DIDs), NFTs or zk-SNARKs. For example: A voting or credential-verification system using Ethereum or Polkadot with built-in proof-of-ownership and audit trail.
		Code Auditing Tools for LLM-Generated Software	Create a tool that audits AI-generated code (e.g., by Copilot or ChatGPT) to detect insecure patterns or unintended behavior. For example: Static analyzer that identifies hardcoded secrets, unsanitized inputs, or bad crypto implementations in generated code snippets.
		Autonomous Threat Hunting with AI Agents	Build AI-driven agents that scan, identify, and flag suspicious behavior in live systems or simulated networks. For example: A bot that navigates logs, extracts indicators of compromise (IOCs), and generates a real-time threat report.
		Cyber Deception & Honeypot Frameworks	Develop adaptive honeypots or deception systems that can lure and analyze adversaries in real time. Example: Create a dynamic honeynet that mimics critical infrastructure and logs attacker behavior.
		Secure Collaboration Platforms for Classified or Sensitive Data	Build an encrypted workspace that supports secure document sharing, messaging, and role-based access controls. Example: A zero-trust collaboration suite for government or military use.

Ministry of Communications and Information Technology

DIGITOPIA

Category	Challenge	Challenge Title	Problem Statement
Graduates up to 35 years old (قائد الأثر)	Resilience & Trust: Advanced Security Innovations	Automated Security Compliance Checker for Cloud Computing Platforms	Design a tool that verifies if systems or cloud configurations comply with national or industry standards (e.g., ISO 27001, NIST). Example: A dashboard that scans and flags noncompliant AWS resources.
		Insider Threat Detection in Hybrid Work Environments	Build behavior-based analytics to detect malicious or negligent internal actors. Example: A machine learning tool that tracks user behavior anomalies across VPN, email, and endpoint logs.
		Cybersecurity for Wearables and Medical IoT Devices	Propose protections for devices like smartwatches, insulin pumps, or remote health trackers. Example: An anomaly detection engine that monitors Bluetooth traffic for medical wearables.
		Zero-Knowledge Proof (ZKP) Applications for Privacy & Trust	Develop systems that leverage ZKPs to prove facts (like identity, access rights, or transaction validity) without revealing underlying data. Example: Build a ZKP-based login system where users can prove they meet access requirements without disclosing their credentials.
		Data Loss Prevention	Design a Data Loss Prevention (DLP) system that identifies and restricts the unauthorized transfer of sensitive data outside the organization. The system should monitor data flows, flag potential breaches, and enforce real-time policies to prevent data exfiltration while ensuring minimal disruption to business operations.
		Secure Software & Service Supply Chain Verification	Develop a system to verify the integrity of software packages, updates, and service components against tampering or malicious injections during the delivery lifecycle. Example: Create a tool that scans and cross-validates hashes, signatures, and provenance metadata of deployed packages and APIs to detect anomalies from within.
		AI Model Watermarking for IP Protection and Attribution	Develop techniques or tools to embed robust, verifiable watermarks in AI models to assert ownership or detect misuse. Example: Create a watermarking system for LLMs that embeds signature traces into output patterns without degrading model performance.

Ministry of Communications and Information Technology

DIGITOPIA

الفئة	التحدي	عنوان التحدي	وصف المشكلة
المرحلة الابتدائية - الصف الرابع إلى الصف السادس (مستكشف الأثر)	أمن بياناتك الصحية	صندوق بيانات المرضى الآمن	إنشاء تطبيق رقمي لتخزين بيانات المرضى بطريقة مشفرة وآمنة.
		محاكاة تفاعلية لممارسات الأمن السيبراني للأطباء	تصميم لعبة لتعليم الطاقم الطبي أفضل ممارسات الأمن السيبراني.
	توفير واجهة مستخدم آمنة	مولد كلمات مرور قوية واختبار قوتها	بناء تطبيق يساعد المستخدمين على إنشاء كلمات مرور قوية واختبارها.
		واجهة صراف آلي آمنة	محاكاة واجهة صراف آلي آمنة تشمل إدخال الرقم السري وتأكيد الهوية.
		لعبة كشف رسائل التصيد الإلكتروني	لعبة تفاعلية تساعد المستخدم على التمييز بين الرسائل الحقيقية ورسائل التصيد.
	تأمين خدماتك الحكومية عبر الإنترنت	تطبيق تسجيل الدخول للخدمات الحكومية	بناء تطبيق تسجيل دخول للمواطنين للخدمات الحكومية باستخدام تقنيات مصادقة بسيطة مثل كلمات المرور، كلمات المرور لمرة واحدة OTP، إلخ.
		نظام امن للتصويت الإلكتروني	إنشاء تطبيق امن للتصويت الاكترونى يسجل كل صوت ويسمح بالمراجعة والتدقيق.
	درع الأمان	روبوتات أو ألعاب التوعية الرقمية	تصميم لعبة تعليمية للجوال أو روبوت محادثة يُعلّم السلوك الآمن على الإنترنت ويقدم نصائح يومية عن الأمان الرقمي
		منصة للمساعدة ضد التحرش والتنمر الإلكتروني	إنشاء منصة إبلاغ دعم مجهولة الهوية تركز على حماية الفئات الضعيفة (مثل الأطفال والنساء)، تتضمن: - إمكانية الإبلاغ الآمن عن الاعتداءات - إحالات إلى خدمات الإرشاد النفسي - موارد تعليمية لمكافحة الاستغلال والتحرش الإلكتروني

Ministry of Communications and Information Technology

DIGITOPIA

الفئة	التحدي	عنوان التحدي	وصف المشكلة
المرحلة الإعدادية والثانوية (صانع الأثر)	أمن بياناتك الصحية	تطبيق تشفير السجلات الطبية	بناء أداة بصرية توضح كيفية حماية التشفير للبيانات الصحية.
		محاكاة هجوم الفدية على المستشفيات	محاكاة هجوم برمجية الفدية الذي يقوم بتشفير الملفات مع توضيح خطوات الاستجابة الموصى بها.
	توفير واجهة مستخدم آمنة	نظام تسجيل دخول متعدد العوامل	بناء نظام تسجيل دخول يستخدم كلمة المرور + كلمة مرور لمرة واحدة OTP وهمية أو مسحًا بيومتريًا.
		قارئ رمز الاستجابة السريعة (QR) مع فلتر احتيال	تطبيق يوضح مسح وتحقق من رموز الدفع QR مع تصفية الرموز المزيفة.
		تطبيق اختبار اختراق المصادقة البيومترية	استكشاف كيفية خداع أنظمة المصادقة البيومترية باستخدام بيانات مزيفة.
	تأمين خدماتك الحكومية عبر الإنترنت	خزينة بيانات المواطنين الآمنة باستخدام تقنية البلوك تشين	بناء محاكاة مبسطة لتقنية البلوك تشين لتخزين بيانات المواطنين بشكل آمن.

Ministry of Communications and Information Technology

DIGITOPIA

الفئة	التحدي	عنوان التحدي	وصف المشكلة
المرحلة الإعدادية والثانوية (صانع الأثر)	درع السلامة على الإنترنت	محقق البصمة الرقمية	استخدم مهاراتك البرمجية لإنشاء لعبة أو اختبار تفاعلي وممتع يساعد اللاعبين على تحديد المعلومات التي يمكن مشاركتها بأمان على الإنترنت، وتلك التي يجب الحفاظ على سريتها.
		إنذار التهديدات السيبرانية	أنشئ مشروعًا ممتعًا يصدر تحذيرًا عند قيامك بشيء غير آمن على جهاز الكمبيوتر. على سبيل المثال: يمكنك محاكاة القيام بشيء محفوف بالمخاطر (مثل استخدام كلمة مرور سهلة أو النقر على رابط مزيف). يشمل المشروع: صوت إنذار أو رسالة تحذير منبثقة. رسالة بسيطة تشرح لماذا ما قمت به غير آمن.
		كاشف الفيروسات	أنشئ لعبة ممتعة تقوم فيها بتدمير أنواع مختلفة من فيروسات الكمبيوتر! تظهر الفيروسات على شكل حشرات مضحكة ومتحركة على الشاشة. يمكنك استخدام "درع سيبراني" أو "ليزر" للقضاء عليها وإيقافها. حاول تحقيق أعلى نتيجة وشاهد اسمك على لوحة المتصدرين!
		العب بأمان	أنشئ منصة تُعلّم الآخرين كيفية اللعب بأمان على الإنترنت! اعرض نصائح مثل: عدم مشاركة الأسماء الحقيقية، استخدام كلمات مرور قوية، وإبلاغ شخص بالغ إذا شعرت أن هناك شيئًا مريبًا. اجعلها ممتعة وسهلة الفهم!
		محاكي التصيد الاحتيالي باللهجة المصرية	بناء اختبار أو تطبيق بسيط لتدريب المستخدمين على اكتشاف رسائل التصيد أو الاحتيال (SMS، بريد إلكتروني، أو منشورات وسائل التواصل الاجتماعي) باستخدام أمثلة وسيناريوهات باللهجة المصرية لضمان فعالية التدريب.
		لعبة التوعية الإعلامية	صمِّم تطبيقًا تفاعليًا أو لعبة تعليمية تُثقف المستخدمين—خصوصًا فئة الشباب—حول كيفية التعرّف على الأخبار المزيفة، والحسابات الآلية (البوتات)، وتقنيات الدعاية، لا سيما على مواقع التواصل الاجتماعي.
		تطبيق رقابة اولياء الامور	تطبيق لمساعدة الآباء في مراقبة وتوعية أطفالهم حول الاستخدام الآمن للإنترنت من خلال: 1- تتبع المواقع المُزارَة (مثل تنبيه الوالدين عند زيارة مواقع إباحية أو غير مناسبة) 2- مراقبة الوقت المُستغرَق في الألعاب أو المواقع الإلكترونية 3- تعزيز العادات الرقمية الصحية

Ministry of Communications and Information Technology

DIGITOPIA

الفئة	التحدي	عنوان التحدي	وصف المشكلة
طلبة الجامعات (مبتكر الأثر)	مستكشفو الفضاء السيبراني: نتعلّم كيف نتفوّق على التهديدات الإلكترونية	منصة استخبارات التهديدات	طوِّر منصة استخبارات تهديدات (TIP) تقوم بتجميع وتحليل وعرض بيانات التهديدات السيبرانية في الوقت الفعلي من مصادر متعددة (مثل المصادر المفتوحة، الإنترنت المظلم، السجلات الداخلية). يجب أن تتيح هذه المنصة لفرق الأمن تحديد التهديدات الناشئة ذات الصلة بالمؤسسة بسرعة، وتعزيز التنبيهات بمعلومات سياقية، وتقديم توصيات تلقائية بشأن إجراءات الاستجابة. تأكّد من أن الحل يوضح قيمة تجارية ملموسة من خلال تقليل زمن الاستجابة للحوادث وتحسين تغطية كشف التهديدات.
	أدوات رقمية لمجتمع أكثر أمانًا	الإبلاغ عن الجرائم بشكل مجهول الهوية	أنشئ منصة آمنة تتيح للمواطنين الإبلاغ عن الجرائم أو السلوكيات المخالفة بشكل مجهول، مع حماية هويتهم باستخدام تقنيات التشفير أو الشبكات اللامركزية.
		خريطة استجابة الطوارئ	طوِّر منصة تفاعلية تعتمد على المجتمع وتعمل في الوقت الحقيقي لرصد الحوادث الطارئة (مثل الحرائق، حوادث السيارات، انهيار المباني... إلخ)، وتربط هذه الحوادث بخدمات الطوارئ المناسبة.
		روبوت دردشة للدعم القانوني ومساندة الضحايا	صمِّم روبوت دردشة يقدّم إرشادات سرية حول الحقوق القانونية، كيفية تقديم الشكاوى، وأماكن الحصول على الدعم للضحايا المتعرضين للجرائم أو الإساءة.

Ministry of Communications and Information Technology

DIGITOPIA

الفئة	التحدي	عنوان التحدي	وصف المشكلة
طلبة الجامعات (مبتكر الأثر)	تتبّع وثقة: حلول تقنية لمكافحة السوق السوداء والتجارة المزوّرة	تطبيق التحقق من أصالة المنتج	طوِّر تطبيقًا للهاتف المحمول للتحقق من أصالة الأدوية باستخدام رموز QR أو الأرقام التسلسلية.
		منصة المبلّغين عن المخالفات	أنشئ أداة آمنة تُمكّن المواطنين أو العاملين من الإبلاغ عن أنشطة السوق السوداء بشكل مجهول الهوية.
		متعقّب ذكي لسلسلة التوريد	طوِّر لوحة تحكم لتتبع حركة البضائع من المصدر حتى نقطة البيع باستخدام تقنية البلوكشين أو إنترنت الأشياء (IoT)
		نظام تنبيهات لسلامة الغذاء	صمِّم نظامًا يُصدر تنبيهات حول المنتجات الغذائية غير الآمنة أو غير المرخّصة استنادًا إلى بلاغات المستخدمين ونتائج التفتيش.
	تروث هاك: الدفاع عن الحقيقة في عصر التزييف العميق والمعلومات المضللة	كاشف التزييف العميق	طوِّر أداة مدعومة بالذكاء الاصطناعي تكتشف مقاطع الفيديو أو الصور او الملفات الصوتية المُعدّلة ، وتُشير إلى احتمالية وجود تزييف عميق (Deepfake) في الوقت الفعلي.
		إضافة للتحقق من صحة المعلومات	أنشئ إضافة للمتصفح أو روبوت دردشة يتحقّق من مصداقية المقالات الإخبارية أو منشورات مواقع التواصل الاجتماعي باستخدام قواعد بيانات موثوقة وتقنيات معالجة اللغة الطبيعية (NLP)
		نظام تتبع حملات المعلومات المضللة ونسبها إلى مصادرها الأصلية	طوِّر لوحة تحكم تعرض انتشار المعلومات المضللة الفيروسية، مع تحديد المصادر، وأنماط التضخيم، والجماهير المستهدفة. على سبيل المثال: تطبيق يكشف السلوك غير الأصيل المنسّق أو التأثير المدعوم من جهات حكومية، من خلال تتبّع أنماط النسخ واللصق في الأخبار وآثار الترجمة الآلية.
		أداة تحليل أنماط التلاعب في المحتوى السردي	أنشئ أداة تحلل تطوّر السرديات المضللة من خلال تتبع أساليب الصياغة اللغوية، والنبرة العاطفية، واستراتيجيات التوقيت على مدى الزمن. وعلى عكس أدوات تتبع المصدر، تركّز هذه الأداة على كيفية قيام الحملات المنسّقة بتغيير الرأي العام أو تحريف الحقائق عبر التكرار، وتوجيه المشاعر، والتركيز الانتقائي على المعلومات. مثال: نظام يعتمد على الخط الزمني يُظهر التكتيكات البلاغية المتكررة أو تغيّر اللغة المستخدمة عبر الحملات المختلفة.

Ministry of Communications and Information Technology

DIGITOPIA

الفئة	التحدي	عنوان التحدي	وصف المشكلة
شباب الخريجين حتى سن 35 سنة (قائد الأثر)	التحمّل والثقة: ابتكارات متقدمة في مجال الأمن السيبراني	أدوات استمرارية الأعمال والتعافي من الكوارث	أنشئ أدوات تخطيط أو محاكاة تساعد الخدمات العامة على الاستعداد للاضطرابات السيبرانية. على سبيل المثال: قم بمحاكاة هجوم فدية على بلدية، وابتكر أداة استجابة تتضمّن أدلة تشغيل (Playbooks) وبروتوكولات بديلة لضمان استمرارية الخدمة.
		أنظمة الحوكمة والمخاطر والامتثال GRC للقطاع المالي	طوِّر أدوات للحوكمة والمخاطر والامتثال GRC مُصمّمة خصيصًا للبنوك والمؤسسات المالية. مثال: لوحة تحكم تدمج بين مراقبة التهديدات في الوقت الفعلي وتطبيق السياسات لصالح المدققين الداخليين.
		أنظمة التوأم الرقمي للأمن السيبراني	صمِّم نموذج توأم رقمي لمحاكاة وتعزيز الأمن للبُنى التحتية الحيوية، مثل محاكاة الهجمات على شبكة كهرباء ذكية لاختبار آليات الدفاع وبروتوكولات المراقبة في الوقت الفعلي.
		تحليل أمني متقدّم للأجهزة والبرمجيات الثابتة	قم بتحليل أو تأمين الأنظمة المدمجة وبرمجيات إنترنت الأشياء الثابتة، بما في ذلك BIOS/UEFI أو الأجهزة المعتمدة على المتحكمات الدقيقة Microcontrollers مثال: استخراج البرنامج الثابت من جهاز ذكي للكشف عن الأبواب الخلفية الخفية، أو كتابة محمّل إقلاع آمن Secure Bootloader لمنع التلاعب بالجهاز.
		التحليل الثابت/الديناميكي للبرمجيات الخبيثة على الهواتف الذكية	صمِّم مجموعة أدوات أو خدمة لتحليل تطبيقات الهاتف المحمول المشبوهة باستخدام فحص الكود الثابت ومراقبة السلوك الديناميكي. مثال: أنشئ بيئة "صندوق الرمل" Sandbox تقوم بتسجيل نداءات النظام والنشاطات الشبكية لتطبيقات أندرويد من أجل اكتشاف الأنماط الخبيثة.
		أنظمة الجيل التالي من الجدران النارية	صمِّم أو حسِّن بنية جدار ناري ذكي قادر على اكتشاف الهجمات المتقدّمة، والتهديدات المشفّرة، والسلوك غير الطبيعي باستخدام الذكاء الاصطناعي وبيانات استخبارات التهديدات في الوقت الفعلي. مثال: أنشئ نموذجًا أوليًا لجدار ناري يتضمّن فحصًا على مستوى الطبقة السابعة L7 وكشفًا للشذوذ مدعومًا بتقنيات التعلم الآلي، وموجّهًا لبيئات المؤسسات الصغيرة والمتوسطة أو البُنى التحتية الحيوية.

Ministry of Communications and Information Technology

DIGITOPIA

الفئة	قطاع التحدي	عنوان التحدي	وصف المشكلة
شباب الخريجين حتى سن 35 سنة (قائد الأثر)	التحمّل والثقة: ابتكارات متقدمة في مجال الأمن السيبراني	بيئات المحاكاة للهجوم والدفاع بين الفريق الأحمر والفريق الأزرق	أنشئ بيئة افتراضية حيث يمكن للفرق أن تتولى أدوار هجومية (الفريق الأحمر) أو دفاعية (الفريق الأزرق) لمحاكاة هجمات إلكترونية واستراتيجيات دفاعية واقعية. على سبيل المثال: إنشاء بيئة شبيهة بـ Capture The Flag (CTF)تحتوي على خوادم معرضة للثغرات، حيث يجب على المدافعين اكتشاف الهجمات، والاستجابة لها، وسد الثغرات، بينما يحاول المهاجمون تصعيد الصلاحيات.
		خصوصية البيانات في عصر الذكاء العام الاصطناعي AGIونماذج اللغة الكبيرة LLMs	اقترح آليات لحماية الخصوصية أو أدوات تدقيق تهدف إلى حماية بيانات المستخدم في بيئات مدعومة بالذكاء الاصطناعي. يمكن أن يشمل ذلك تطوير نظام وصول إلى البيانات يراعي موافقة المستخدم، أو اختبار طبقة حماية تعتمد على الخصوصية التفاضلية لتفاعلات المستخدم مع نماذج اللغة الكبيرة LLMs
		أطر أمنية متكاملة للمدن الذكية	صمِّم لوحة تحكم لإدارة الأمن أو نظام تنبيهات ذكي يختص بمكوّنات المدن الذكية مثل إشارات المرور، خدمات المرافق، وأنظمة المراقبة بالفيديو CCTV بحيث يتيح رصد التهديدات والاستجابة لها بشكل فوري. على سبيل المثال، يمكن تطوير محرّك لاكتشاف التهديدات المرتبطة بإنترنت الأشياء ضمن الشبكات البلدية لرصد الأنشطة غير المألوفة وتنبيه الفرق المعنية.
		تأمين أنظمة النقل الذكية	اقترح تدابير للأمن السيبراني تستهدف منصات النقل الذكية مثل شبكات الاتصال بين المركبات والبنية التحتية V2I أو أنظمة التحصيل الآلي للرسوم، وذلك من خلال تصميم حلول تضمن سلامة البيانات وتمنع التلاعب أو التسلل. كمثال تطبيقي، يمكن إنشاء نموذج أولي لنظام كشف التسلل يستهدف عقد الاتصال في شبكات V2X لرصد الأنشطة غير الطبيعية وحماية تدفق البيانات في الوقت الفعلي.
		إطار مصادقة باستخدام التشفير الكامل المتجانس	طور نظام مصادقة يعتمد على التشفير الكامل المتجانس Fully Homomorphic Encryption لإجراء التحقق من الهوية أو فحوصات التحكم في الوصول دون فك تشفير بيانات المستخدم الحساسة. مثال: نظام تسجيل دخول قائم على السحابة يمكنه التحقق من هوية المستخدمين مع الحفاظ على تشفير كامل لبيانات الاعتماد الخاصة بهم طوال العملية.
		بروتوكولات التشفير المقاومة للحوسبة الكمومية	قم بتطوير أو اختبار أنظمة تشفير مقاومة لتهديدات الحوسبة الكمومية. على سبيل المثال، نفذ نموذج تشفير هجين يستخدم خوارزميات قائمة على الشبكات متكاملة مع البنية التحتية الحالية للمفاتيح العامة.

Ministry of Communications and Information Technology

DIGITOPIA

الفئة	التحدي	عنوان التحدي	وصف المشكلة
شباب الخريجين حتى سن 35 سنة (قائد الأثر)	التحمّل والثقة: ابتكارات متقدمة في مجال الأمن السيبراني	مكافحة الهندسة العكسية في البرمجيات ونماذج الذكاء الاصطناعي	قم بإنشاء طبقات حماية أو تقنيات تشويش لجعل الأمر أكثر صعوبة على الخصوم في فك تشفير البرامج المجمعة أو نماذج التعلم الآلي. مثال: بناء نموذج أولي يضيف ميزات مقاومة للتصحيح anti-debugging وتقنيات تشويش للكود لتطبيق ذكاء اصطناعي حساس مكتوب بلغة بايثون.
		التحقق الآمن من الهوية في بيئات البلوكشين والأنظمة اللامركزية	طور نظام إدارة هوية يحافظ على الخصوصية باستخدام المعرفات اللامركزية (DIDs)، أو الرموز غير القابلة للاستبدال NFTs، أو تقنيات zk-SNARKs. مثال: نظام تصويت أو تحقق من الشهادات يعتمد على شبكات مثل إيثيريوم أو بولكادوت مع إثبات ملكية مدمج وسجل تدقيق.
		أدوات تدقيق الكود للبرمجيات المُنتجة بواسطة نماذج اللغة الكبيرة	طور أداة تدقيق للكود المولَّد بواسطة الذكاء الاصطناعي (مثل Copilot أو ChatGPT) تهدف إلى اكتشاف الأنماط غير الآمنة أو السلوك غير المقصود. على سبيل المثال: محلل ثابت (Static Analyzer) يحدد الأسرار المدمجة صلباً في الكود، أو الإدخالات غير المعقمة، أو تطبيقات التشفير الضعيفة في مقاطع الكود المولَّدة.
		الصيد التهديدي المستقل باستخدام وكلاء الذكاء الاصطناعي	قم بتطوير وكلاء مدعومين بالذكاء الاصطناعي يقومون بمسح الأنظمة الحية أو الشبكات المحاكاة لاكتشاف السلوكيات المشبوهة والإبلاغ عنها. على سبيل المثال: بوت يتصفح سجلات النظام، يستخرج مؤشرات الاختراق IOCs، ويولد تقرير تهديدات في الوقت الحقيقي.
		إطارات عمل الخداع السيبراني ونقاط الاصطياد (الهوني بوت)	طور أنظمة خداع أو نُقاط اصطياد (honeypots) قابلة للتكيف تجذب الخصوم وتقوم بتحليلهم في الوقت الفعلي. مثال: إنشاء شبكة اصطياد ديناميكية تحاكي البنية التحتية الحيوية وتسجل سلوك المهاجمين.
		منصات التعاون الآمن للبيانات المصنفة أو الحساسة	قم ببناء بيئة عمل مشفرة تدعم مشاركة المستندات بشكل آمن، والتراسل، والتحكم في الوصول بناءً على الأدوار. مثال: مجموعة تعاون تعتمد على مبدأ "عدم الثقة" (Zero-Trust) مخصصة للاستخدام الحكومي أو العسكري.
		مدقق تلقائي للامتثال الأمني لمنصات الحوسبة السحابية	صمم أداة تتحقق مما إذا كانت الأنظمة أو إعدادات السحابة متوافقة مع المعايير الوطنية أو الصناعية (مثل ISO 27001، NIST) مثال: لوحة تحكم تقوم بفحص موارد AWS وتحديد الموارد غير المتوافقة.

Ministry of Communications and Information Technology

DIGITOPIA

الفئة	التحدي	عنوان التحدي	وصف المشكلة
شباب الخريجين حتى سن 35 سنة (قائد الأثر)	التحمّل والثقة: ابتكارات متقدمة في مجال الأمن السيبراني	اكتشاف تهديدات الداخل في بيئات العمل الهجينة	طور تحليلات قائمة على السلوك لاكتشاف الجهات الداخلية الخبيثة أو المهملة. مثال: أداة تعلم آلي تتابع شذوذات سلوك المستخدم عبر سجلات الشبكة الافتراضية الخاصة (VPN)، والبريد الإلكتروني، ونقاط النهاية.
		الأمن السيبراني للأجهزة القابلة للارتداء وأجهزة إنترنت الأشياء الطبية	اقترح وسائل حماية للأجهزة مثل الساعات الذكية، ومضخات الإنسولين، أو أجهزة تتبع الصحة عن بُعد. مثال: محرك لاكتشاف الشذوذ يراقب حركة مرور البلوتوث للأجهزة الطبية القابلة للارتداء.
		تطبيقات إثبات المعرفة الصفرية (ZKP) للخصوصية والثقة	طوّر أنظمة تستفيد من تقنيات إثبات المعرفة الصفرية (ZKPs) لإثبات حقائق مثل الهوية، أو صلاحيات الوصول، أو صحة المعاملات دون الكشف عن البيانات الأساسية. مثال: إنشاء نظام تسجيل دخول يعتمد على ZKPيتيح للمستخدمين إثبات استيفائهم لمتطلبات الوصول دون الإفصاح عن بيانات اعتمادهم.
		منع فقدان البيانات	صمّم نظامًا لمنع فقدان البيانات (DLP) يقوم بتحديد ومنع نقل البيانات الحساسة بشكل غير مصرح به خارج المؤسسة. يجب أن يراقب النظام تدفقات البيانات، ويرصد أي انتهاكات محتملة، ويطبّق سياسات فورية لمنع تسريب البيانات، مع ضمان الحد الأدنى من التأثير على سير العمليات التشغيلية.
		التحقق الآمن من سلسلة توريد البرمجيات والخدمات	طوّر نظامًا للتحقق من سلامة حزم البرمجيات، والتحديثات، ومكونات الخدمات ضد أي تلاعب أو حقن خبيث أثناء دورة تسليمها. مثال: أنشئ أداة تقوم بفحص والتحقق المتقاطع لقيم التجزئة hashes، والتواقيع الرقمية، وبيانات مصدر المنشأ provenance metadata للحزم والتطبيقات البرمجية APIs المثبتة، بهدف اكتشاف أي شذوذ أو تغييرات من الداخل.
		الوسم المائي لنماذج الذكاء الاصطناعي لحماية الملكية الفكرية ونسب المصدر	طوّر تقنيات أو أدوات لإدراج علامات مائية قوية وقابلة للتحقق داخل نماذج الذكاء الاصطناعي لإثبات الملكية أو كشف سوء الاستخدام. مثال: إنشاء نظام وسم مائي للنماذج اللغوية الكبيرة (LLMs) يدمج بصمات رقمية داخل أنماط الإخراج دون التأثير على أداء النموذج.

Egypt’s AI's future starts with you!

Connect with us and let's build it together!

DIGITOPIA

Apply Now

Ministry of Communications and Information Technology

www.digitopia.gov.eg

Contact Us:

info-CS@digitopia.gov.eg

Hotline:

15110