



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy



المخيم الشبابي للأمن السيبراني

التقرير التنفيذي



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المخيم الشبابي للأمن السيبراني

التقرير التنفيذي



المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026



مقدمة

يهدف المخيم الصيفي للشباب في مجال الأمن السيبراني إلى إعداد جيل واعد يمتلك المهارات والمعرفة اللازمة في هذا التخصص الحيوي منذ سن مبكر، عبر تمكين الطلاب من استكشاف مسارات مهنية ناجحة من خلال برامج تدريبية متكاملة، إلى جانب رفع مستوى الوعي بأهمية الأمن السيبراني وتعزيز شبكة العلاقات والتواصل بين المشاركين.

ورش تفاعلية

جلسات عملية تُترجم المفاهيم إلى تطبيق مباشر.

تطبيقات عملية

تدريبات حقيقية في بيئة آمنة ومحفزة.

محاضرات مع خبراء

نقاش مباشر مع نخبة من المختصين المعتمدين.

الرؤية

استقطاب ورعاية الشباب الموهوبين في مجال الأمن السيبراني، وتنمية قدراتهم ومهاراتهم لتمكينهم من المساهمة الفاعلة في بناء مستقبل رقمي آمن.

الرسالة

استقطاب واحتضان الشباب الموهوب في الأمن السيبراني، وتنمية مواهبه ومهاراته بما يهيئه لمستقبل مهني واعد.



الأهداف

1 تمكين الطلاب من التأهيل الأكاديمي للالتحاق بكليات ومعاهد تكنولوجيا المعلومات والأمن السيبراني، وزيادة فرصهم في سوق العمل.

2 تقديم تجربة تدريبية مبتكرة تمزج بين الجانبين النظري والعملي بأساليب تفاعلية جذابة.

3 استخدام أدوات وأساليب تعليمية حديثة تعتمد على الترفيه والتحديات والابتكار لتعزيز الفهم وتحفيز الإبداع.

4 تعزيز روح الفريق والعمل الجماعي بين المشاركين من خلال الأنشطة التفاعلية والمسابقات التنافسية.

5 تعزيز المهارات العملية والاحترافية في مجال الأمن السيبراني بما يهيئ المشاركين للتميز في مساراتهم المستقبلية.

6 اكتشاف المواهب السيبرانية الشابة وتوجيهها نحو المسارات المناسبة، والمساهمة في إعداد كوادر وطنية مؤهلة.



الفئة المستهدفة

طالب وطالبة من القطريين والمقيمين، ذكوراً وإناثاً، بأعمار 17-13 عاماً، من المدارس الحكومية والخاصة في دولة قطر.

400



التعلم عن بعد

طالب وطالبة شاركوا عن بعد من مختلف دول العالم.

1000



توقيت المخيم

الإناث: الأحد-الخميس، 8:00 ص - 12:30 م

الذكور: الأحد-الخميس، 1:00 م - 5:00 م

ثلاثة أسابيع

19 يوليو - 6 أغسطس

الشركاء

وزارة الرياضة والشباب
Ministry of Sports and Youth
دولة قطر • State of Qatar



وزارة التربية والتعليم والتعليم العالي
Ministry of Education and Higher Education
دولة قطر • State of Qatar



ooredoo

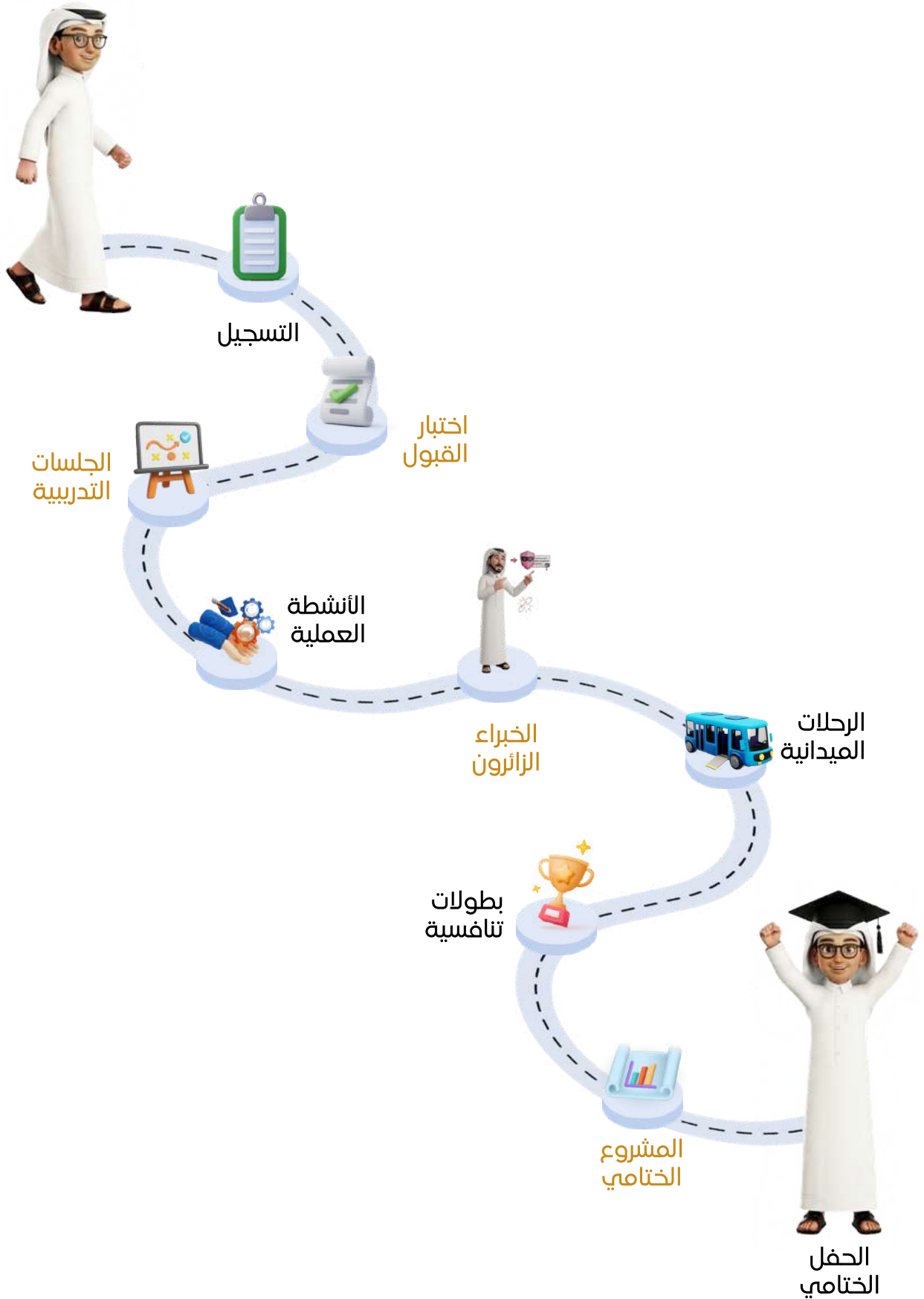


مدرسة قطر للعلوم والتكنولوجيا الثانوية للبنين
Qatar Science & Technology Secondary School for Boys



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

رحلة الطالب



الأنشطة الترفيهية والإثرائية



صنع الخُلي



الرسم على المرايا



حل لغز الجريمة



الهروب من الفيروس



الرياضات اللاسلكية



ورشة صناعة الشموع



تحدي بناء سيارة



مسابقة CTF التقاط العلم - تحدي Bank Breach

تحدٍ عملي يختبر مهارات الطلبة في الاختراق الأخلاقي من خلال حل تحديات تقنية واستغلال الثغرات ضمن سيناريوهات واقعية، بما يعزز مهاراتهم في التحليل والعمل الجماعي واتخاذ القرار تحت ضغط الوقت.

مطاردة

ثم اختراق خادم مجموعة القرصنة نفسها لإنهاء المهمة.

استرداد

على الطلاب إعادة اختراق البنك لاستعادة السيطرة عليه.

اختراق

مجموعة قرصنة من «الدارك ويب» تمكنت من اختراق البنك المركزي.

الهدف

وضع الطلاب في موقف واقعي يطبقون فيه ما تعلموه في جمع المعلومات والاختراق ضمن إطار قانوني آمن، من الاستطلاع حتى السيطرة الكاملة على الهدف، وصقل روح الفريق واتخاذ القرار تحت ضغط الوقت.



الزيارات الميدانية - شركة أوريدو



تم تنظيم زيارة ميدانية إلى المقر الرئيسي لشركة Ooredoo، شارك خلالها الطلاب في ورشة متخصصة في الأمن السيبراني، تعرّفوا من خلالها على أهمية المجال وأبرز مساراته المهنية، بالإضافة إلى أدوار فرق الأمن السيبراني داخل المؤسسات، مثل إدارة المخاطر والامتثال، وهندسة الأمن، ومركز العمليات الأمنية (SOC)، مما أسهم في ربط المعارف النظرية بالتطبيقات المهنية الواقعية.

الخبراء



ضمن برنامج المخيم، تُنظَّم جلسات تفاعلية يلتقي فيها المشاركون مباشرةً بنخبة من خبراء الأمن السيبراني من مختلف القطاعات، حيث يشاركونهم خبراتهم العملية ورؤاهم المهنية. تتيح هذه الجلسات للطلاب طرح الأسئلة وطلب النصائح واكتساب معرفة مهنية وتقنية قيّمة، بما يُعزِّز فهمهم لمفاهيم الأمن السيبراني ويهيئهم لمساراتهم المستقبلية في المجال.

المحتوى التدريبي

ينقسم المحتوى التدريبي إلى ستة موضوعات رئيسية:

القرصنة الأخلاقية	الويب	الأساسيات
الدفاع السيبراني	النظم	الشبكات

يتم تناولها من خلال:



الدفاعات

تعلم كيفية الحماية من الهجمات وتخفيف آثارها.



الهجمات

تعلم كيفية الهجوم والتسوية لفهم أساليب المهاجمين.



الأساسيات

تعلم المفاهيم الأساسية للأمن السيبراني وبناء أرضية معرفية متينة.



أدوات التعلم

المنصة

منصة TryHackMe هي بيئة تعلم تفاعلية مصممة لتعزيز مهارات الأمن السيبراني من خلال التدريب العملي. توفر المنصة مختبرات افتراضية ودورات تدريبية تفاعلية، مما يتيح للمستخدمين اكتساب خبرة عملية في التعامل مع سيناريوهات الأمن السيبراني المختلفة.



الكتيب

كتيب شامل لاحتواء كافة مخيم الأمن السيبراني، إلى جانب بعض الأنشطة الترفيهية الممتعة. يوفر هذا الكتيب مرجعاً شاملاً للمشاركين، ليتمكنوا من استرجاع المعلومات القيمة والأنشطة التفاعلية، والتحديات الشيقة التي مروا بها خلال المخيم.



التدريب أونلاين — بُعد يتجاوز القاعة

رافق المخيم الحضوري بثّ تدريبي "أونلاين" مفتوح، عُقد على هيئة ندوتين تفاعليتين يوميًا (صباحية ومساءلية) تغطيان موضوعات المخيم نفسها. أتاح هذا البُعد لمن هم خارج المقاعد الحضورية المحدودة متابعة المحتوى والتفاعل المباشر مع المدربين.

11

دولة حول العالم

20

ندوة تفاعلية
(صباحية ومساءلية)

1,165

إجمالي الحضور عبر الندوات

أضاف البُعد الأونلاين أكثر من 1,000 حضورٍ جديدٍ إلى أثر المخيم، من 11 دولة حول العالم.

مشاريع التخرج - رحلة المشروع

تمثل مرحلة مشاريع التخرج مرحلة محورية في المخيم، حيث أتاحت للطلبة فرصة تطبيق المعارف والمهارات التي اكتسبوها خلال فترة التدريب وتحويلها إلى مشاريع عملية. كما ساهمت هذه المرحلة في تعزيز مهارات العمل الجماعي، وحل المشكلات، والتفكير الإبداعي، وربط الجانب النظري بالتطبيق العملي في مجال الأمن السيبراني.

رحلة المشروع



أبرز المحاور التي توزعت عليها المشاريع

التعليم والمحاكاة التفاعلية

منصات تحوّل التعلّم إلى تجربة عملية، Admins، Operation Shadow، Case Files.

كشف الاحتيال والتصيّد

أدوات موحّدة تفحص الروابط والرسائل والصور المزيفة، Cyberderaa، منصة حصن، Cyberdreams.

الدفاع المتقدم وحماية البيانات

مصائد ذكية وحماية بيانات المؤسسات، RansomLab، حصن الغاز، QSecure.

حماية الملفات والأجهزة

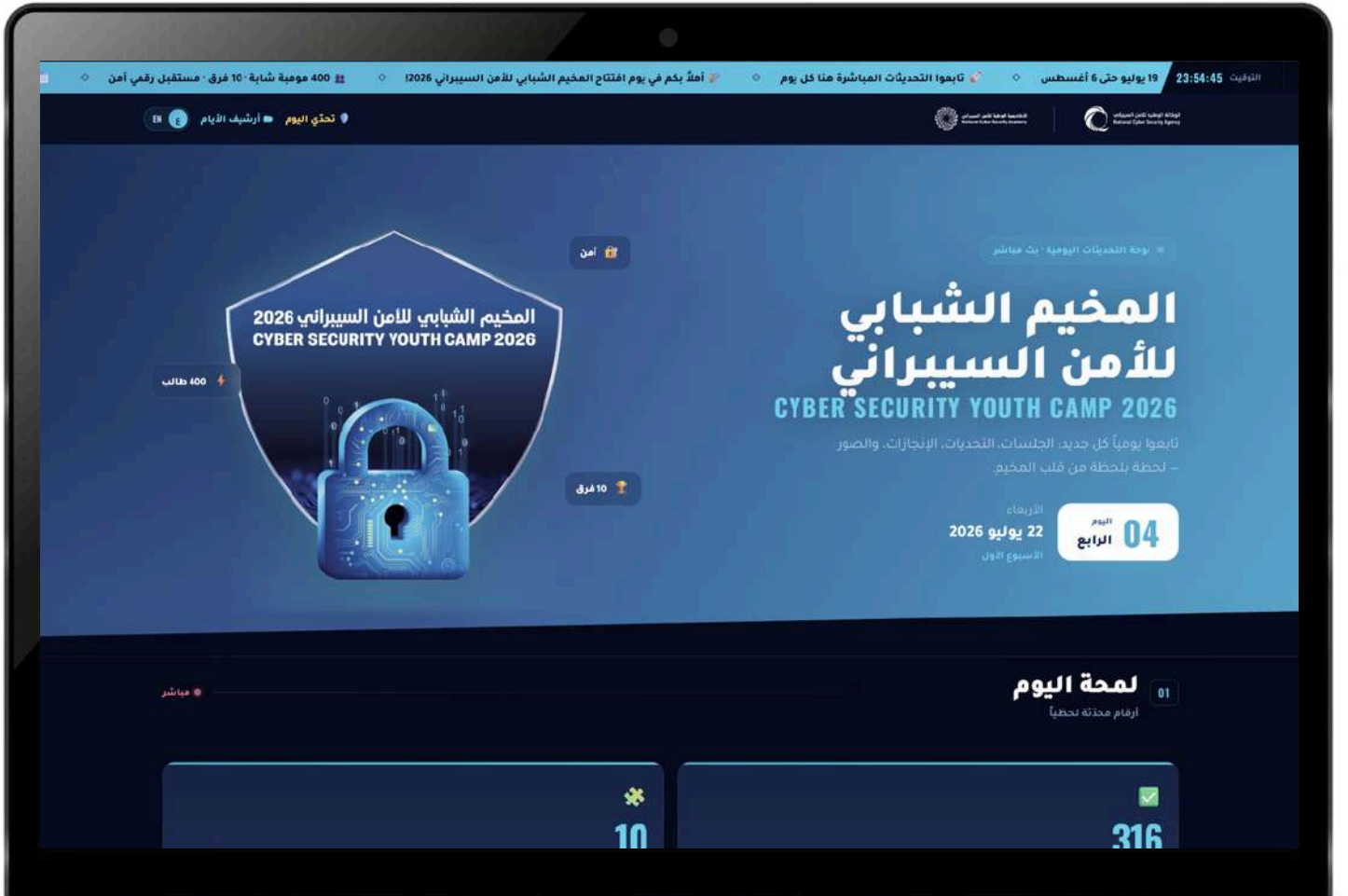
مراقبة سلامة الملفات وفحص وسائط USB، HexaGuard، FileShield، StegoVault.

منصة التحديثات اليومية

صُمّمت المنصة لتكون لوحة حية تفاعلية لا موقعًا تقليديًا ثابتًا، حيث يتضمّن:

- جدول الحصص التعليمية المباشر لأربع مجموعات مختلفة، يمكن التنقل بينها بضغطة واحدة.
- بيانات حضور ونقاط تتحدّث ذاتيًا من جدول بيانات إلكتروني.
- لوحة تحكم دون الحاجة إلى كتابة أكواد برمجية، لتستخدم من قبل المنظمين.
- تحدي يومي تفاعلي.
- أرشيف كامل يوثق فعاليات كل يوم.

وقد أسفر ذلك عن انخفاض ملحوظ في مكالمات أولياء الأمور منذ الأسبوع الأول، وتحول حقيقي من حالة القلق إلى متابعة يومية يتشاركها الأهالي فيما بينهم.



الحفل الختامي



مشاريع التخرج لطلاب المخيم الشبابي للأمن السيبراني

خلال المخيم الشبابي للأمن السيبراني تم تطوير مشاريع تخرج تختص بمجالات متعددة تتعلق بالأمن السيبراني و في إطار الحفل الختامي، أُتيحت فرصة لأفضل 20 مشروع تخرج العرض أمام أولياء الأمور والشركاء والضيوف، بمشاركة الفئتين العمريتين (13-14 سنة) و(15-17 سنة).

تنوعت المشاريع في عدد من مجالات الأمن السيبراني، شملت أمن الشبكات، والقرصنة الأخلاقية، والدفاع السيبراني، وأمن تطبيقات الويب، وعكست مستوى المهارات والمعارف العملية التي اكتسبها الطلاب وطوّروها خلال أسابيع المخيم الثلاثة.

كما شكّل المعرض منصة لتمكين الطلاب من عرض أفكارهم بما يعكس المخرجات العملية للمخيم وأثره في تطوير مهارات المشاركين في مجال الأمن السيبراني.

- 80 مشروع تخرج يختص في مجالات مختلفه في الأمن السيبراني.
- 20 مشروع تخرج مؤهلين للنهائيات.
- فئتان عمريتان: 13-14 و 15-17 سنة.
- 4 مجالات رئيسية في الأمن السيبراني.



العرض المسرحي وفيديو رحلة المخيم

استعرض الفيديو أبرز مراحل رحلة الطلاب خلال المخيم، من التدريب والأنشطة العملية والتحديات، وصولاً إلى تطوير مشاريع التخرج والمشاركة في الحفل الختامي، موثقاً تجربة الطلاب والمهارات والخبرات التي اكتسبوها خلال فترة البرنامج.



مسرحية : من الشغف بالألعاب الى المسؤولية الوطنية

قدّم الطلاب عرضاً مسرحياً يجسّد الانتقال من الشغف بالتكنولوجيا والألعاب إلى الوعي بأهمية الأمن السيبراني والمسؤولية الرقمية. وعكس العرض أبرز القيم والرسائل التي ركّز عليها المخيم، مثل الوعي الرقمي، والاستخدام الآمن والإيجابي للتكنولوجيا.



تكریم الفرق الفائزة بأفضل مشاريع تخرج

المركز الأول



عدد الطلاب المكرمين: 8
الجائزة: Iphone 17



الفرق الفائزة:
Admins, Black Hats

المركز الثاني



عدد الطلاب المكرمين: 8
الجائزة: Iphone 17



الفرق الفائزة:
Cyberderaa, Sanad

المركز الثالث



عدد الطلاب المكرمين: 8
الجائزة: Iphone 17



الفرق الفائزة:
Operation Shadow, Conquest



إحصائيات المخيم



15

موضوعات أساسية



1000

مشارك عن بعد



349

مشارك حضوري



6

تحديات سيبرانية



8

خبراء زائرين



25

مدرب



15

يوماً من الأنشطة



80

مشروع تخرج



4

زيارات ميدانية



50

ساعة من التدريب



4

شركاء

التغذية الراجعة حسب ملاحظات الطلاب والمشرفين

التنظيم والتجربة العامة: إشادة بمستوى التنظيم وتجربة المخيم بشكل عام، مع مقترحات لتحسين توزيع أوقات الحصص والاستراحات والأنشطة.

المدربون والإداريون: رضا عن تعاون المدربين والإداريين ودعمهم للمشاركين، مع تقدير أسلوب الشرح والتعامل والمتابعة.

المحتوى والتطبيق العملي: اهتمام واضح بالمحتوى السيبراني، مع رغبة في زيادة التطبيقات العملية والتحديات CTF وتقليل الجانب النظري.

الأنشطة والمسابقات: تفاعل إيجابي مع الأنشطة الترفيهية والجماعية، مع مطالب بزيادتها وإضافة أنشطة رياضية وحركية ومسابقات أكثر بين الصفوف.

الأنشطة التفاعلية: إعجاب بالتجارب العملية مع اقتراحات لإطالة زمن الأنشطة وإضافة فعاليات جديدة.

التطوير المستقبلي: أبدى المشاركون اهتمامًا بأنشطة جديدة تشمل الرياضة، والتحديات السيبرانية العملية، والألعاب الجماعية، والأعمال اليدوية والرحلات.

آراء المشاركين في المخيم

"هذه السنة الثالثة لي في مخيم الأمن السيبراني، وفي كل عام ألاحظ تطورًا واضحًا في جودة المحتوى والمعلومات المقدمة. استمتعت كثيرًا بتجربتي في المخيم، وكانت تجربة إيجابية لدرجة أنني شجعت أقاربي على التسجيل والمشاركة فيه."

- الطالب حمد محمد المحشادي المعاضيد



"هذه أول مرة أشارك فيها في مخيم الأمن السيبراني، وسجلت فيه بناءً على توصية من أقاربي. استفدت كثيرًا من المعلومات والمهارات التي تعلمتها خلال البرنامج، وكانت بالنسبة لي تجربة مميزة وثرية."

- الطالب فهد حمد المري



"أكثر ما أعجبني في المخيم أنه يجمع بين التعلّم والأنشطة والألعاب التي تساعدنا على البقاء متيقظين ومركزين، بالإضافة إلى الاهتمام بالتقييم في نهاية كل أسبوع."

- الطالبة عائشة طارق الخاطر



"أكثر ما أعجبني في المخيم هم المنظمون، فقد كانوا متعاونين ومتواجدين دائمًا للمساعدة. كما أعجبتني الأنشطة لتنوعها ومتعتها واختلاف كل فعالية عن الأخرى، مما جعل تجربتي في المخيم جميلة ومميزة."

- الطالبة لولو ناصر الكواري



آلية تبني الموهوبين



مشاريع التخريج



اسم المشروع: Admins - الفائز بالمركز الأول (13-14)

نبذة عن المشروع

منصة تعليمية تفاعلية للأمن السيبراني موجّهة للطلاب الشغوفين الذين يفتقرون إلى مخيمات أو مدارس متخصصة. تعتمد منهجية تطبيقية عبر موقع إلكتروني يقرن كل درس نظري بتحدّي عملي واقعي في بيئة ويب آمنة، فينتقل الطالب من الحفظ النظري إلى ممارسة مهارات الأمن السيبراني فعلياً وبوتيرة تناسب مستواه.

المخرجات:

- منصة ويب تعليمية بدروس تفاعلية.
- تحديات عملية بمحتوى واقعي مباشر.
- مسارات ذاتية الوتيرة لكل مستوى.
- بيئة تدريب آمنة دون مخيمات أو مدارس.

الأهداف:

- منح الطلاب الشغوفين تدريباً عملياً حقيقياً.
- سد فجوة غياب المخيمات والمدارس المتخصصة.
- تحويل المعرفة النظرية إلى ممارسة فعلية.



اسم المشروع : Admins

أعضاء الفريق: Mariam Almousa, Menna Gabr, Joudy Hasanen, Aisha Al-Rabban

الحل

الحل هو إنشاء منصة تعليمية رقمية في مجال الأمن السيبراني، توفر محتوى تفاعلي وتحديات عملية، بحيث تُمنح الطلاب فرصةً للتعلّم والتدريب دون الحاجة إلى مخيمات أو مدارس خاصة.

The solution is to create a digital learning platform in cybersecurity that offers interactive content and practical challenges, giving students opportunities to learn

المنهجية

يعتمد المشروع على منهجية تطبيقية من خلال تطوير موقع إلكتروني يقدم تحديات في الأمن السيبراني، بهدف مساعدة الطلاب والمهتمين على ممارسة المعارف النظرية في بيئة واقعية آمنة باستخدام تقنيات ويب حديثة.

The project follows an applied methodology by developing a web platform with cybersecurity challenges, aiming to help students and enthusiasts practice theoretical knowledge in real-world scenarios using modern web technologies.

التحدي

هناك عدد كبير من الطلاب لديهم شغف بمجال الأمن السيبراني، إلا أنهم يفتقرون إلى الفرص المناسبة للانخراط بالمخيمات الصيفية أو المدارس المتخصصة في هذا المجال.

There are a large number of students who have a passion for the field of cybersecurity, but they lack the right opportunities to attend summer camps or specialized schools in this field.



المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

فريق المشروع: مريم حسن الأحمد أحمد موسى ، منة محمد جبر، جودي سامح حسنين، عائشة محمد الريان

اسم المشروع: سند - الفائز بالمركز الثاني (13-14)

نبذة عن المشروع

سند منصة ذكية لحماية الأطفال من الابتزاز والاستدراج والتنمر الرقمي، ترصد الخطر لحظة وقوعه بدل التوعية العامة المتأخرة. يحل محرك الكشف الرسائل عبر قاعدة كلمات خطرة في خمس فئات مقرونة بتحليل السياق بالكاء الاصطناعي، فيصنّف الحالة عبر مؤشر واضح (آمن/مشبوه/خطير/حرج) ويبلّغ ولي الأمر فوراً، مع خصوصية تامة دون تخزين بيانات الطفل.

المخرجات:

- محرك كشف: كلمات خطرة وتحليل سياق ذكي.
- مؤشر خطورة: آمن/مشبوه/خطير/حرج.
- تنبيه فوري لولي الأمر عند الخطر.
- لعبة توعية وواجهة عربية وإنجليزية.

الأهداف:

- حماية الأطفال من الابتزاز والاستدراج والتنمر.
- رصد الخطر لحظة وقوعه لا بعد فواته.
- كسر صمت الطفل بتنبيه فوري للأسرة.

اسم المشروع: Sanad

أعضاء الفريق: صيته عامر الحميدي، ريم سحيم الجلابي، أمته سحيم الجلابي، حصه عبدالرحمن عبدالله

الحل

- منصة ذكية تحمي الأطفال رقمياً:
- تحليل ذكي للابتزاز والاستدراج والتنمر والاحتيال.
- تفسير النتيجة لا مجرد تحذير.
- مؤشر: آمن / مشبوه / خطير / حرج.
- تنبيه فوري لولي الأمر.
- لعبة تفاعلية لبناء الوعي.
- خصوصية تامة بلا تخزين.

سند
SANAD
الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المنهجية

- 1 تحديد المشكلة
أسئلة رئيسية المخاطر والوعي.
- 2 قاعدة البيانات
نظمنا خطرة في 5 فئات
- 3 محرك الكشف
كلمات - تحليل السياق بالذكاء الاصطناعي
- 4 بناء المنصة
واجهة عربية وإنجليزية واحدة لها علم
- 5 التنبيه
تنبيه فوري لولي الأمر
- 6 التقييم
قياس أكثر بأستبيات

التحدي

1. تعرّض الأطفال يومياً للابتزاز والاستدراج والتنمر والاحتيال الإلكتروني.
2. ضعف الوعي الرقمي بعلامات الخطر وطرق التصرف الصحيح.
3. الطفل لا يميز المحال إلا بعد وقوع الضرر.
4. انوات التوعية التقليدية تافهة، ولا ترصد الخطر لحظة حدوثه.
5. المطلق يصمت خوفاً، فيعلم ولي الأمر متأخراً!

الهدف من المشروع: حماية الأطفال من الابتزاز والاستدراج والتنمر الإلكتروني.

الهدف من المشروع: حماية الأطفال من الابتزاز والاستدراج والتنمر الإلكتروني.

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

فريق المشروع: صيته عامر الحميدي، ريم سحيم الجلابي، أمته سحيم الجلابي، حصه عبدالرحمن عبدالله

اسم المشروع: Conquest - الفائز بالمركز الثالث (13-14)

نبذة عن المشروع

Conquest موقع تعليمي مجاني يساعد المبتدئين على إتقان أدوات Kali Linux دون إرهاق أمام كثرة الخيارات. يرتب الأدوات ضمن ثلاثة فرق متخصصة (Red/Blue Team) وحالات استخدام واضحة، ويربط كل أداة بأمر جاهز وشرح مبسط لمتى ولماذا تُستخدم، فيتدرب الطالب عملياً على أدوات مثل Burp Suite John the Ripper Gobuster Hydra Nmap.

المخرجات:

- موقع يضم 14 أداة و42 أمراً جاهزاً.
- تصنيف الأدوات في 3 فرق (Red/Blue).
- أوامر جاهزة: Hydra Nmap Gobuster.
- شرح مبسط لمتى وكيف تُستخدم كل أداة.

الأهداف:

- تسهيل حفظ أوامر Kali Linux للمبتدئين.
- توضيح متى وكيف تُستخدم كل أداة.
- إتاحة تعلم عملي مجاني بالكامل.

اسم المشروع: Conquest

أعضاء الفريق: عبدالله حمد السفران، سلطان سالم السفران، علي سالم النعيمي

التحدي

يواجه الطلاب المبتدئون في الأمن السيبراني صعوبة في:

- حفظ أوامر أدوات Kali Linux.
- معرفة متى وكيف يتم استخدام كل أداة.
- التنقل بين عدد كبير من الأدوات والمراجع.
- التعلم بطريقة عملية وسهلة.

المنهجية

لقد أنشأنا موقعاً إلكترونياً يساعد المبتدئين على التعامل مع الأدوات بسهولة وبساطة الوصول إليها.



1. بدء المستخدم: بدأ الطالب رحلته في التعلم مع Conquest.
2. فتح برنامج Conquest: يتم تحميل البرنامج على نظام Kali Linux.
3. اختبار أداة: يختار الطالب أداة التي يريدها من بين أدوات Red Team أو Blue Team.
4. عرض البرنامج: يعرض البرنامج الأوامر الخاصة بالأداة التي اختارها الطالب، مع شرح مبسط لكل أمر.
5. شرح مبسط: يوفر البرنامج شرحاً مبسطاً لكل أداة، مع أمثلة عملية.
6. تدريب الطالب: يتدرب الطالب على الأوامر التي تعلمها، مع دعم فني متاح في أي وقت.

الحل

ما هو منهجنا؟

Conquest هو منهج يجعل البرمجة أسهل وأكثر كفاءة. ويتميز بما يلي:

- يحتوي على 14 أداة.
- يعتمد على 3 فرق عمل بتخصصات مختلفة.
- يضم 42 أمراً جاهزاً لتسهيل العمل.
- التعلم مجاني بالكامل (0 تكلفة).



المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

فريق المشروع: عبدالله حمد السفران، سلطان سالم السفران، علي سالم النعيمي

اسم المشروع: Black Hats - الفائز بالمركز الأول (15-17)

نبذة عن المشروع

Black Hats مشروع يُبرز خطورة البرمجيات الخبيثة وصعوبة اكتشافها بطريقة آمنة ومضبوطة بالكامل. بنى الفريق محاكاة فعلية بلغة Python لأنواع شائعة , Ransomware و RAT و Keylogger. لغرض تعليمية بحثية, مستعيناً بـ kimi AI لتحديد البرمجيات الخبيثة و DeepSeek AI لفهم شيفرتها, ثم استخلص عادات عملية تقلل احتمال الإصابة.

المخرجات:

- محاكاة بلغة Python لأنواع خبيثة شائعة.
- نماذج: Ransomware و RAT و Keylogger.
- تحليل الشيفرة بـ kimi AI و DeepSeek AI.
- إرشادات تحديث ونسخ احتياطي وحماية.

الأهداف:

- توضيح خطورة البرمجيات الخبيثة وصعوبة كشفها.
- بناء محاكاة آمنة لأغراض تعليمية بحثية.
- تعليم عادات عملية تقلل الإصابة.

اسم المشروع: Black Hats

أعضاء الفريق: فهد الخاطر, أحمد فضل الله, علي الذوايدي, عبد الله المحمود

التحدي

مع تزايد استخدام التقنية في حياتنا اليومية, لا يزال وعي الكثير من أفراد المجتمع بمخاطر البرمجيات الخبيثة محدوداً. لا يدرك الكثيرون أن البرمجيات الخبيثة قد تُعرض بياناتهم وخصوصيتهم للخطر في لحظات, مما يجعل التوعية ضرورة لا خياراً. هدف مشروعنا هو التوعية بمدى خطورة هذه البرمجيات وصعوبة الكشف عنها عند الإصابة بها.

المنهجية

يشتمل المشروع منهجية منظمة تضمن إجراء محاكاة آمنة مع تحقيق الأهداف التوعوية في بيئة معزولة وآمنة.

استخدمنا kimi AI لتحديد لبناء البرمجيات الخبيثة, كما استخدمنا Deepseek AI لمساعدتنا في فهم الـ code بشكل أفضل.

تم كتابة الملف بلغة python حيث يحتوي على برامج خبيثة وهي:

- Ransomware
- Remote Access Trojan
- Keylogger

الحل

لحماية أجهزتنا من البرمجيات الضارة, يجب:

- تحديث نظام التشغيل والبرامج باستمرار لسد الثغرات الأمنية التي قد يستغلها المهاجمون
- استخدام برامج حماية موثوقة
- إنشاء نسخ احتياطية منتظمة للملفات المهمة
- عدم فتح الروابط المشبوهة أو مجهولة المصدر
- عدم استخدام أجهزة USB أو External drive غير آمنة

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

فريق المشروع: علي عبدالله الذوايدي, فهد عبدالله الخاطر, عبدالله جاسم المحمود, احمد فضل الله عوضي

اسم المشروع: Cyberderaa - الفائز بالمركز الثاني (15-17)

نبذة عن المشروع

Cyberderaa أداة موحّدة تجمع كشف الصور المزيفة وفحص الروابط والنصوص المشبوهة في مكان واحد، مقترنة بمساعد سيبراني تفاعلي لرفع وعي المستخدم اليومي. طوّرت كتطبيق ويب بلغة Python/Flask مرتبط بواجهات APIs متخصصة: Hive Moderation لكشف الصور المزيفة، وVirusTotal لفحص الروابط، وGemini AI لتحليل النصوص، فتتحقق بسرعة ودقة مما هو آمن للنقر.

المخرجات:

- فحص موحّد للصور والروابط والنصوص.
- تطبيق ويب Python/Flask مرتبط بـ APIs.
- Gemini AI وVirusTotal وHive Moderation.
- مساعد سيبراني يرصد الرسائل المشبوهة.

الأهداف:

- التصدي للتزايد السريع في الاحتيال الرقمي.
- كشف الصور المزيفة المولّدة بالذكاء الاصطناعي.
- تسهيل التحقق السريع من الروابط والنصوص.

اسم المشروع: Cyberderaa

أعضاء الفريق: فلاك راشد، الهام الهاشمي، موزة جبر، الدانة منصور

الحل

فحص فوري موحد للصور والروابط والنصوص، مع مساعد سيبراني تفاعلي لتوعية المستخدمين وتحليل الرسائل المشبوهة



المنهجية

تطبيق ويب (Python/Flask) مرتبط بـ APIs للتحقق:

- Hive Moderation: لكشف الصور المزيفة.
- VirusTotal: لفحص الروابط.
- Gemini AI: لتحليل النصوص.



التحدي

- تزايد الاحتيال
- تزايد الصور المزيفة المولدة بالذكاء الاصطناعي.
- صعوبة التحقق من سلامة الروابط والنصوص





الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

فريق المشروع: الدانة منصور سالم النعيمي، موزة جبر محمد جاسم آل ثاني، فلاك راشد فهد الدوسري، الهام عبدالمجيد الهاشمي

اسم المشروع: Operation Shadow - الفائز بالمركز الثالث (15-17)

نبذة عن المشروع

Operation Shadow منصة محاكاة تفاعلية تضع المستخدم في دور محلل أمني يواجه هجوماً سيبرانياً متصاعداً من التصيد حتى سرقة البيانات. يحدّد كل قرار، صائباً أو خاطئاً، مسار الهجوم ونتائجه فعلياً، بدعم خريطة شبكة حيّة ومساعد ذكي (SHADOW AI) وتقييم نهائي يوضّح الأداء. منصة ويب سهلة تعمل عبر المتصفح وبدون إنترنت وقابلة للتوسّع للمؤسسات.

المخرجات:

- محاكاة كاملة: من التصيد إلى سرقة البيانات.
- قرارات المستخدم تغيّر مسار الهجوم.
- خريطة شبكة حيّة ومساعد SHADOW AI.
- منصة ويب تعمل بلا إنترنت وقابلة للتوسّع.

الأهداف:

- إبراز الخطأ البشري كسبب رئيسي للاختراقات.
- استبدال التوعية النظرية بتجربة واقعية.
- تمكين اتخاذ قرارات حقيقية أثناء الهجوم.

اسم المشروع: Operation Shadow

أعضاء الفريق: لطيفه الحنزاب، نجود المالك، عايشه المري

التحدي

- تزايد الهجمات السيبرانية، ويُعد الخطأ البشري السبب الرئيسي لنجاح معظم الاختراقات.
- تعتمد برامج التوعية الحالية على أساليب نظرية لا تُعدّ الموظفين للتعامل مع الهجمات الفعلية.
- غياب حلول تدريبية تفاعلية وأمنة تمنح المستخدم تجربة واقعية لاتخاذ القرارات أثناء الهجوم.

المنهجية

- تطوير محاكاة تفاعلية لهجوم سيبراني متكامل تبدأ بالتصيد الاحتمالي وتنتهي بمحاولة سرقة البيانات.
- إشراك المستخدم في دور محلل أمني لاتخاذ قرارات تؤثر مباشرة على سير الهجوم ونتائجه.
- دعم التجربة بخريطة شبكة حيّة، ومساعد ذكي (SHADOW AI)، وتقييم نهائي يوضح الأداء وتأثير القرارات.

الحل

- منصة "عملية الظل" تحول التوعية الأمنية من محتوى نظري إلى تجربة تفاعلية تحاكي الهجمات السيبرانية.
- تمكّن المستخدم من التعلّم بالممارسة ورؤية تأثير قراراته مباشرة، مع تقييم يوضح نقاط القوة والضعف.
- منصة سهلة الاستخدام، تعمل عبر المتصفح وبدون اتصال بالإنترنت، وقابلة للتوسّع لتناسب المدارس والجامعات والشركات.

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

فريق المشروع: نجود علي المالك، لطيفه الحنزاب

اسم المشروع: Case Files

نبذة عن المشروع

Case Files لعبة سيبرانية تفاعلية تحوّل تعلّم الأمن السيبراني إلى تجربة تحقيق جنائي رقمي حيّة. يتفكّص الطالب دور محقق سيبراني يستلم قضية اختراق حقيقية، فيجمع الأدلة الرقمية ويحلّل الخيوط ويتجاوز تحديات التقاط الأعلام (CTF) ليكتشف كيف تسلّل المهاجم، ثم يبنّي خطة وقائية ويحصل على شهادة إنجاز، فيعيش نتائج القرارات الأمنية بدل حفظ الحقائق.

المخرجات:

- رحلة تحقيق: قضية وأدلة وتحديات CTF.
- بناء خطة وقائية قبل إغلاق القضية.
- نظام تقييم مع شهادة إنجاز رقمية.
- محاكاة تهديدات: تصيد وكلمات مرور ضعيفة.

الأهداف:

- توعية الطلاب بمخاطر التصيد وضعف كلمات المرور.
- استبدال التلقين بتعلّم عملي تفاعلي.
- تدريب مهارات التحقيق وتحليل الأدلة الرقمية.

CASE FILES : اسم المشروع

أعضاء الفريق: فاطمة الأنصاري، شهد محسن، نعيمة محمد الباهلي، الجازي الكواري

Every clue matters. Every decision counts

The Problem

Students use technology every day, but many are unaware of cybersecurity risks.

Common threats include phishing, weak passwords, fake websites, and online scams.

Traditional learning often focuses on theory instead of hands-on experience.

Our Methodology

How It Works

Mission: Receive a cyberattack case.

Investigate: Collect and analyse digital evidence.

Solve: Complete cybersecurity challenges and capture flags.

Prevent: Create a security plan to stop future attacks.

Achieve: Complete the case and earn a certificate.

The Solution

CASE FILES is an interactive cybersecurity game where students become cyber investigators.

Players collect evidence, analyse clues, solve challenges, and create a prevention plan while learning how cyberattacks happen and how to stop them.

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

فريق المشروع: فاطمة الأنصاري، شهد محسن، نعيمة محمد الباهلي، الجازي الكواري

اسم المشروع: Cyberdreams

نبذة عن المشروع

Cyberdreams منصة شاملة تستخدم الذكاء الاصطناعي لتحليل الروابط ورسائل البريد ورموز QR دفعة واحدة، وتقيّم خطورة كل منها مع نصائح حماية قابلة للتطبيق. تجمع ست أدوات منفصلة , محلل تصيد ومحلل QR ومحلل بريد ومحلل خصوصية المواقع ومركز تعلم ومولّد كلمات مرور , في لوحة واحدة, فيستغني المستخدم عن التنقل بين تطبيقات متعددة, وتُحفظ نتائج التحليل لعرضها لاحقاً.

المخرجات:

- تحليل ذكي للروابط والرسائل ورموز QR.
- ست أدوات متكاملة في لوحة واحدة.
- محلل تصيد وخصوصية مواقع ومولّد كلمات مرور.
- تقارير فورية مع سجل تحليل محفوظ.

الأهداف:

- التصدي للانتشار المتزايد لهجمات التصيد.
- تسهيل التحقق من الروابط والرسائل المشبوهة.
- رفع الوعي الأمني بأدوات سهلة الاستخدام.

اسم المشروع: Cyberdreams

أعضاء الفريق: الجوري العتيبي, المها الهيال, هيا العبدالله

الحل

- 1- محلل روابط التصيد الإحتيالي
- 2- محلل رموز الاستجابة السريعة (QR)
- 3- محلل البريد الإلكتروني
- 4- محلل خصوصية المواقع الإلكترونية
- 5- مركز التعلم
- 6- مولد كلمات المرور

المنهجية

يقوم المستخدم بإدخال رابط أو رسالة بريد إلكتروني أو رمز (QR) أو سؤال. يقوم النظام بتحليل البيانات باستخدام الذكاء الاصطناعي. يحدد مستوى الخطورة. يقدم تقريراً ونصائح لحماية المستخدم. يحفظ نتائج التحليل لعرضها لاحقاً.

التحدي

- 1- إنتشار هجمات التصيد الإلكتروني . (phishing)
- 2- صعوبة التحقق من الروابط و رسائل البريد الإلكتروني المشبوهة
- 3- نقص الوعي الأمني لدى المستخدمين

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

فريق المشروع: الجوري عبدالعزيز العتيبي, المها خالد الهيال, هيا جعيش العبدالله

اسم المشروع: HexaGuard

نبذة عن المشروع

HexaGuard نظام دفاعي يراقب أجهزة USB المتصلة تلقائياً ويحلل ملفات قبل أن يفتح المستخدم أي شيء عليها. بدل التخمين، ينشئ النظام بصمة رقمية (SHA-256) لكل ملف ويقارنها بقاعدة تهديدات VirusTotal، ثم يحسب درجة خطورة واضحة عبر محرك كشف متعدد التقنيات ويعرض توصية عملية قابلة للتنفيذ، مع حفظ كل النتائج في سجل فحص (Scan History).

المخرجات:

- اكتشاف تلقائي لأجهزة USB وفحص ملفات.
- بصمة SHA-256 لكل ملف قبل فتحه.
- مقارنة VirusTotal ودرجة خطورة محسوبة.
- سجل فحص يوثق النتائج والتوصيات.

الأهداف:

- تقييم خطورة ملفات USB قبل فتحها.
- أتمتة الفحص بدل الاعتماد على التخمين.
- تقديم توصية أمنية واضحة وعملية.

اسم المشروع: HexaGuard

أعضاء الفريق: رايه عبدالله المهندي، دانة عبدالقادر بابكر، أمل فاطمة

الحل

HexaGuard هو نظام دفاعي يقوم بمراقبة أجهزة التخزين القابلة للإزالة وتحليل الملفات الموجودة عليها باستخدام تقنيات متعددة، ثم يعرض تقريراً يوضح مستوى الخطورة ويوفر توصيات تساعد المستخدم على اتخاذ القرار المناسب.

المنهجية

- اكتشاف جهاز USB المتصل.
- فحص الملفات الموجودة على الجهاز.
- إنشاء بصمة رقمية (SHA-256) لكل ملف.
- مقارنة البصمة مع قاعدة بيانات VirusTotal.
- حساب درجة الخطورة باستخدام محرك تقييم المخاطر.
- عرض تقرير ورسالة توصية للمستخدم.
- حفظ نتائج الفحص في سجل Scan History.

التحدي

تعد أجهزة التخزين القابلة للإزالة مثل وحدات USB وسيلة شائعة لنقل الملفات، لكنها قد تشكل خطراً أمنياً بسبب إمكانية احتوائها على ملفات ضارة أو غير متوقعة. يحتاج المستخدم إلى وسيلة تساعد على تقييم مستوى خطورة هذه الملفات قبل استخدامها.

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

فريق المشروع: رايه عبدالله المهندي، دانة عبدالقادر بابكر، أمل فاطمة

اسم المشروع: QSecure

نبذة عن المشروع

QSecure منصة مصائد إلكترونية ذكية (QAHN) تعمل داخل شبكة المؤسسة وتغيّر هويتها باستمرار باستخدام توليد الأرقام العشوائية الكمية (QRNG)، ما يجعل اكتشافها أو توقعها أصعب بكثير من المصائد التقليدية. تعيد باستمرار تشكيل بصمة نظام التشغيل وصفحات الدخول والمنافذ المفتوحة والملفات الوهمية عبر محرك تكيف، وتعيد ضبط نفسها تلقائياً عند رصد نشاط مشبوه.

المخرجات:

- منصة QAHN مصائد داخل شبكة المؤسسة.
- QRNG يعيد تشكيل المصيدة باستمرار.
- منافذ وصفحات دخول وملفات وهمية متغيرة.
- إعادة ضبط تلقائية عند رصد نشاط مشبوه.

الأهداف:

- معالجة سهولة اكتشاف المصائد الثابتة.
- بناء مصيدة أذكى وأقدر على التكيف.
- زيادة عدم القابلية للتنبؤ بخصائصها.

اسم المشروع: Qsecure

أعضاء الفريق: عائشة طارق الخاطر، شهد محمد قاسم، فجر علي العمادي

الحل

- تغيير هوية الخادم باستمرار.
- منافذ وخدمات ديناميكية.
- صفحات تسجيل دخول متنوعة.
- ملفات وهمية تتغير باستمرار.
- استخدام QRNG لزيادة عدم قابلية التنبؤ.

المنهجية

- منصة برمجية متخصصة QAHN تعمل داخل شبكة المؤسسة لحماية أنظمتها من الهجمات الإلكترونية.
- توليد أرقام عشوائية باستخدام مولد الأرقام العشوائية الكمية (QRNG).
- إرسال القيم إلى محرك التكيف.
- تغيير خصائص المصيدة بشكل مستمر، مثل:
 - نظام التشغيل.
 - صفحة تسجيل الدخول.
 - المنافذ المفتوحة.
 - الملفات والخدمات الوهمية.
 - عند اكتشاف نشاط مشبوه، يعيد النظام تغيير إعداداته تلقائياً لإرباك المهاجم.

التحدي

- يستطيع المهاجمون اكتشاف (Honeytrap) من خلال تحليل المنافذ المفتوحة، ونظام التشغيل، وسلوك الخادم.
- عند اكتشافها، يتوقف المهاجم عن التفاعل معها، مما يقلل من المعلومات التي يحصل عليها فريق.
- مع تطور الهجمات الإلكترونية، أصبحت الحاجة إلى مصائد أكثر ذكاءً وتكيفاً ضرورية.

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

فريق المشروع: عائشة طارق الخاطر، شهد محمد قاسم، فجر علي العمادي

اسم المشروع: منصة حصن

نبذة عن المشروع

منصة حصن منصة موحّدة تعتمد الذكاء الاصطناعي لفحص الروابط والرسائل ورموز QR والصور وسياسات الخصوصية وتقييم خطورتها في مكان واحد، بدل التنقل بين أداة منفصلة لكل تهديد. تحلّل المحتوى بنماذج ذكاء اصطناعي وقواعد بيانات موثوقة، فتحدّد نوع التهديد ومستواه، وتعرض معاينة آمنة للروابط، وتلخّص سياسات الخصوصية بلغة مبسّطة، مع مساعد ذكي ووضوح طوارئ للاستجابة الفورية.

المخرجات:

- فحص موحّد: روابط ورسائل وQR وصور.
- معاينة آمنة للروابط وكشف الصور المزيفة.
- تلخيص سياسات الخصوصية بلغة مبسّطة.
- مساعد ذكي ووضوح طوارئ للاستجابة.

الأهداف:

- تجميع أدوات الحماية المتفرقة في منصة واحدة.
- تسريع الاستجابة بدل تشتت الانتباه.
- تمكين القرار الصحيح قبل أي تفاعل رقمي.

اسم المشروع: حصن

أعضاء الفريق: فاطمة جعفري، حصة النعيمي، وضحه المري، ليلي أشكناني، فاطمه المالكي

الحل

منصة حصن الذكية توفر للمستخدم مجموعة من أدوات الحماية في مكان في مكان واحد، وتشمل:

- فحص الروابط مع عرض معاينة آمنة لمحتواها
- فحص رموز QR واكتشاف الروابط الضارة قبل فتحها
- تحليل الرسائل الذي للكشف عن رسائل التصيد والاحتيال
- التحقق من أصالة المحتوى وكشف الصور المزيفة
- حماية خصوصية الصور عن إزالة البيانات الخفية
- تحليل وتلخيص سياسات الخصوصية للمواقع بلغة مبسطة
- مساعد ذكي يقدم إرشادات وتوعية أمنية فورية
- الإبلاغ عن عمليات الاحتيال لدعم رفع الوعي
- وضع الطوارئ الذي يوفر إرشادات فورية وخطوات الاستجابة عند الاشتباه بالتعرض لهجوم أو اختراق

المنهجية

تم تطوير منصة حصن بالاعتماد على منهجية تجمع بين تقنيات الذكاء الاصطناعي وأدوات تحليل الأمن السيبراني في منصة موحدة

- تستقبل المنصة مخلات المستخدم: (روابط، رسائل، QR، صور، سياسات الخصوصية)
- يتم تحليل المحتوى باستخدام نموذج ذكاء اصطناعي وقواعد بيانات آمنة موثوقة وأدوات متقدمة
- يتم تقييم مستوى الخطورة وتحديد نوع التهديد واحتمالية
- تقديم نتائج فورية مدعومة بتوصيات واضحة وإرشادات عملية لمعالجة المستخدم
- تمكين المستخدم من اتخاذ القرار الصحيح قبل التفاعل مع أي محتوى رقمي

التحدي

مع التطور المتسارع للهجمات السيبرانية، أصبح المستخدم يواجه تهديدات متنوعة مثل:

- روابط التصيد والاحتيال
- رموز QR الخبيثة
- الرسائل الاحتمالية والهندسة الاجتماعية
- الصور المزيفة والمحتوى المزيف
- سياسات الخصوصية المعقدة
- الحاجة لاستخدام أدوات متعددة ومتفرقة للتحقق من كل تهديد

النتيجة:

هذا التثقيف يقلل من سرعة الاستجابة ويزيد من احتمالية الوقوع ضحية للهجمات الإلكترونية

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

فريق المشروع: فاطمة عيسى شعبان جعفري، حصة منصور النعيمي، وضحه محمد راشد المري، ليلي أشكناني، فاطمه حسين المالكي

اسم المشروع: حصن الغاز

نبذة عن المشروع

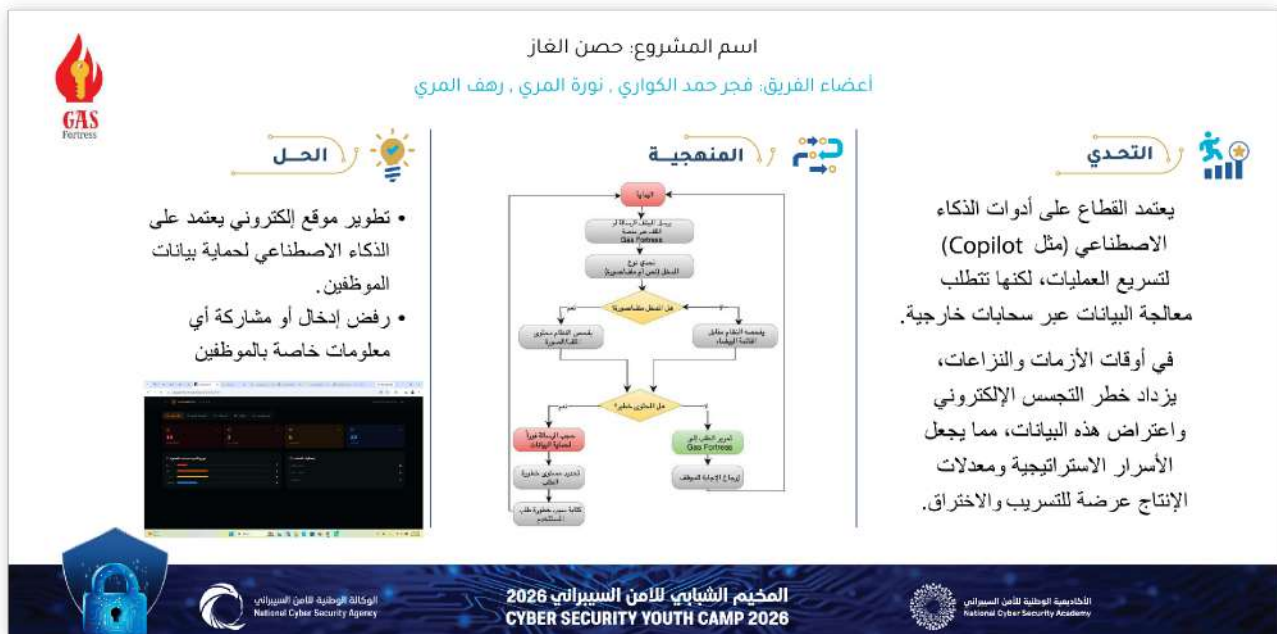
حصن الغاز موقع يعتمد الذكاء الاصطناعي لحماية بيانات موظفي قطاع الغاز من التسريب خلال الأزمات والمخاطر الجيوسياسية، حين يشتد الاعتماد على أدوات ذكاء اصطناعي خارجية (مثل Copilot) تعالج البيانات عبر سحابت خارجية. يفحص النظام كل رسالة أو ملف مقابل قائمة بيضاء ويحلل محتواه، فيحجب الحساس فوراً أو يعزّره مع تحديد مستوى خطورته وسببه، لحماية الأسرار الاستراتيجية وأرقام الإنتاج.

المخرجات:

- موقع بالذكاء الاصطناعي يحمي بيانات الموظفين.
- فحص المدخلات مقابل قائمة بيضاء.
- حجب فوري للبيانات الحساسة وقت الخطر.
- تحديد مستوى الخطورة وسببه لكل طلب.

الأهداف:

- تقليل الاعتماد على السحابت الخارجية للبيانات.
- حماية الأسرار الاستراتيجية وبيانات الإنتاج.
- تعزيز الأمن السيبراني وقت الأزمات.



فريق المشروع: ريف صالح علي، ال سفران المري، فجر حمد الكواري، نورة صالح المري

اسم المشروع: Cyber Falcons

نبذة عن المشروع

Cyber Falcons منصة متكاملة تجمع عدة أدوات أمنية كانت منفصلة في مكان واحد لتحليل البرمجيات الخبيثة وفحص الروابط. تدعم أنواعاً مختلفة من الملفات، وتتيح للمستخدم اختبار المدة الواقعية لكسر كلمة مروره واختبار وعيه بالتصيد، مع محتوى تعليمي وفيديوهات من مصادر عالمية. طوّرت عبر مراحل منظّمة: تحليل المتطلبات فالتصميم فالتطوير فالاختبار فالنشر والتقييم.

المخرجات:

- منصة متكاملة لتحليل البرمجيات وفحص الروابط.
- دعم تحليل أنواع مختلفة من الملفات.
- اختبار زمن كسر كلمة المرور والوعي بالتصيد.
- محتوى تعليمي وفيديوهات من مصادر عالمية.

الأهداف:

- دمج عدة أدوات أمنية في منصة واحدة.
- تحسين الأداء لعمل المشروع بسلاسة.
- تكامل مكونات المشروع ومعالجة الأخطاء.



فريق المشروع: صالح راشد العذبه، فهد مسفر المري، سلطان فهد المهندي، محسن نايف الشمري

اسم المشروع: FileShield

نبذة عن المشروع

FileShield أداة تراقب الملفات الحساسة باستمرار وتكتشف أي تعديل غير مصرّح به لحظة حدوثه عبر بصمة رقمية (SHA-256) موقعة بعبارة مرور. بدل اكتشاف الاختراق بعد أشهر عبر فحص يدوي بطيء، يحصل المستخدم على تنبيه فوري لأربع حالات: التعديل أو النسخ أو الحذف أو إعادة التسمية. طوّرت بلغة JavaScript/React عبر VSCode Claude بلوحة حية عربية وإنجليزية.

المخرجات:

- كشف فوري لأربع حالات تغيير للملف.
- بصمة SHA-256 موقعة بعبارة مرور.
- لوحة مراقبة حية عربية وإنجليزية.
- بُنيت بـ JavaScript/React عبر Claude وVSCode.

الأهداف:

- كشف التعديل على الملفات فوراً لا لاحقاً.
- استبدال الفحص اليدوي بمراقبة آلية.
- ضمان سلامة الملفات الحساسة والتحقق منها.

اسم المشروع: FileShield

أعضاء الفريق: يوسف احمد عبيدالله، محمد سلمان العامري، علي سالم المري

الحل

- الكشف الفوري لأربع حالات
- بصمة SHA-256 موقعة بعبارة مرور
- مراقبة حية بلغة عربية وإنجليزي



المنهجية

- استخدمنا كلاود مع Vscode
- استخدمنا لغة البرمجة Javascript / react
- اعتمدنا بصمة SHA-256 مرجعا للمقارنة

التحدي

- ملفات حساسة تعدل دون أن يلاحظ أحد
- الاكتشاف يأتي بعد أشهر من الضرر
- الفحص اليدوي للملفات مستحيل



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

فريق المشروع: يوسف احمد عبيدالله، محمد سلمان العامري، علي سالم صالح السفيران المري

اسم المشروع: HOMAND

نبذة عن المشروع

HOMAND منصة موحدة تبحث عن الهوية الرقمية المبعثرة للمستخدم عبر نحو 65 منصة في آن واحد، وتشغل 18 أداة أمنية احترافية بالتوازي مع تحقق مدعوم بالذكاء الاصطناعي من النتائج فور ورودها. بدل التحقق يدوياً من عشرات المواقع في ساعات مع تفويت حسابات مكشوفة، يحصل المستخدم على تقرير حيّ سهل القراءة خلال دقائق، للاستخدام التعليمي المصّح به فقط.

المخرجات:

- بحث آلي في نحو 65 منصة بالتوازي.
- تشغيل 18 أداة أمنية احترافية معاً.
- تحقق بالذكاء الاصطناعي بنتائج حيّة.
- تقارير محفوظة سهلة القراءة خلال دقائق.

الأهداف:

- توحيد البحث عن الهوية عبر عشرات المنصات.
- استبدال التحقق اليدوي بفحص مدعوم بالذكاء.
- دمج أدوات أمنية معقدة في منصة سهلة.

اسم المشروع: HOMAND

أعضاء الفريق: حسن ماجد العلي، سالم محمد المري، خالد سامي اليافعي، عبد العزيز عبد الله السليطي

الحل

- منصة ويب واحدة سهلة
- بحث عن الهوية + ذكاء اصطناعي
- 18 أداة أمنية احترافية
- استخدام تعليمي مصّح به فقط



المنهجية

- البحث في 65 منصة دفعة واحدة
- تأكيد الهوية بالذكاء الاصطناعي
- تشغيل 18 أداة أمنية بتوازي
- نتائج حيّة وتقارير محفوظة



التحدي

- حسابات الشخص مبعثرة على منصات كثيرة
- أدوات منفصلة ومعقدة
- تأكيد الهوية يدوي ويستغرق ساعات
- لا توجد منصة موحدة





الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

فريق المشروع: حسن ماجد العلي، سالم محمد المري، خالد سامي اليافعي، عبد العزيز السليطي

اسم المشروع: IRSHAAD

نبذة عن المشروع

IRSHAAD منصة توعية تفاعلية لنشر ثقافة أمن سيبراني حقيقية بين الأطفال والكبار عبر دروس مبسطة وأدوات عملية واختبارات تفاعلية بدل المواد التقنية الكثيفة. تضم مجموعة أدوات تفاعلية (نحو 30 أداة) وخريطة تهديدات حية وفاحص تسريب البريد ومختبر تصيد، مع مساعد ذكاء اصطناعي مدمج يجب فور طرح السؤال، ونظام تقييم داخلي يتابع تقدّم كل مستخدم بمرور الوقت.

المخرجات:

- منصة بدروس وأدوات واختبارات تفاعلية.
- نحو 30 أداة: تحليل روابط وكلمات مرور.
- خريطة تهديدات حية وفاحص تسريب البريد.
- مساعد ذكاء اصطناعي ونظام تتبّع للتقدّم.

الأهداف:

- تعزيز وعي جميع الأعمار بالتصيد والاحتيال.
- تصميم محتوى يناسب مختلف الفئات العمرية.
- تقديم مساعدة فورية بالذكاء أثناء التعلّم.

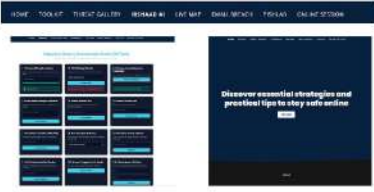
اسم المشروع: IRSHAAD

أعضاء الفريق: حمد احمد المحشادي، سيف علي سعيد
البريص، محمد سالم المحمد، خالد محمد الرشيد

الحل

IRSHAAD Cybersecurity Awareness

هي منصة تعليمية تفاعلية تهدف إلى نشر ثقافة الأمن السيبراني لدى الأطفال والكبار، من خلال دروس مبسطة، أدوات عملية، واختبارات تفاعلية تساعد المستخدم على اكتساب مهارات الحماية الرقمية بطريقة ممتعة وسهلة.



المنهجية

- 1 دراسة أكثر التهديدات السيبرانية انتشارًا.
- 2 تصميم محتوى تعليمي يناسب مختلف الفئات العمرية.
- 3 تطوير منصة تفاعلية تضم أدوات تعليمية واختبارات.
- 4 دمج تقنيات الذكاء الاصطناعي لتقديم المساعدة الفورية.
- 5 تقييم أداء المستخدم وقياس تقدمه من خلال التحديات والأنشطة.

التحدي

مع تزايد استخدام الإنترنت، يواجه الأطفال والكبار مخاطر سيبرانية مثل التصيد الإلكتروني وسرقة الحسابات والاحتيال الرقمي، مما يستدعي تعزيز الوعي بالأمن السيبراني عبر وسائل تعليمية تفاعلية وسهلة الاستخدام.

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

فريق المشروع: حمد احمد المحشادي، سيف علي سعيد البريص، محمد سالم المحمد،
خالد محمد الرشيد

اسم المشروع: Phish Guard AI

نبذة عن المشروع

Phish Guard AI أداة تستخدم الذكاء الاصطناعي لتحليل الرسائل والإيميلات والصور المشبوهة وتحديد احتمال كونها تصيداً مع شرح واضح للسبب. بدل الاعتماد على الشكل الظاهري، تستخرج النص من الصور عبر OCR، وتفحص أنماط الكلمات المشبوهة (Urgent/Verify/Free)، وتفحص الروابط المضمنة بحثاً عن نطاقات مزيفة، ثم تمنح درجة خطورة من 0 إلى 100 مع لعبة تعليمية (Phishing or Not).

المخرجات:

- درجة خطورة من 0 إلى 100 مع تفسير.
- استخراج نص من الصور عبر OCR.
- فحص أنماط الكلمات والروابط المشبوهة.
- لعبة تعليمية (Phishing or Not Battle Mode).

الأهداف:

- التصدي للانتشار الواسع لهجمات التصيد.
- تمييز الرسائل المزيفة بشكل موثوق.
- رفع الوعي بهجمات البريد والصور.

اسم المشروع: Phish Guard Team

أعضاء الفريق: مشعل المفتاح، علي الفضالة

الحل

منصة Phish Guard AI
تحليل الرسائل والإيميلات والصور
تحديد مستوى الخطورة (آمن / حذر / مشبوه)
شرح سبب التصنيف للمستخدم تقديم
نصائح للحماية
لعبة تعليمية (Phishing or Not+ Battle Mode)

المنهجية

استخدام الذكاء الاصطناعي لتحليل النصوص
والصور فحص الروابط واكتشاف النطاقات المزيفة
تحليل الكلمات المشبوهة مثل (Urgent/ Verify / Free)
استخراج النص من الصور (OCR) وتحليله
إعطاء درجة خطورة من 0 إلى 100
بناء لعبة تفاعلية لزيادة الوعي

التحدي

انتشار هجمات التصيد الاحتيالي بشكل
كبير
صعوبة تمييز الرسائل المزيفة من
الحقيقية
اعتماد المستخدمين على الشكل بدل
التحقق من المصدر
زيادة الهجمات عبر البريد الرسائل والصور
ضعف الوعي بالأمن السيبراني



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

فريق المشروع: مشعل سعود المفتاح، علي محمد الفضالة

اسم المشروع: StegoVault

نبذة عن المشروع

StegoVault أداة تُخفي الرسائل الحساسة داخل صور تبدو عادية باستخدام خوارزمية LSB، دون أي فرق مرئي بين الصورة الأصلية والحاملة للرسالة، وبلا حاجة لأي اتصال إنترنت. تعمل محلياً بالكامل وتدعم صيغ JPEG و PNG عبر واجهة بسيطة بخطوتين (اختر الصورة ثم استخرج الرسالة)، وصُممت لحالات قد يلفت فيها الإرسال العلني الانتباه: الصحفيون والنشطاء والمؤسسات.

المخرجات:

- إخفاء الرسائل بخوارزمية LSB دون فرق مرئي.
- عمل محلي بالكامل دون حاجة لإنترنت.
- دعم صيغ JPEG و PNG بواجهة بخطوتين.
- صورة حاملة مطابقة للأصل جاهزة للمشاركة.

الأهداف:

- إخفاء المعلومات أثناء إرسالها دون لفت انتباه.
- تجاوز ضعف أدوات الإخفاء التقليدية.
- حماية الصحفيين والنشطاء من اعتراض الرسائل.

اسم المشروع: StegoVault

أعضاء الفريق: حمد عبدالهادي المري، عبدالله حمد الحنزاب، فيصل طارق أحمد الكشادي، مشعل ضيف الله مرجان غازي الجاسم

مميزات StegoVault

- إخفاء الرسائل في خطوة واحدة داخل تطبيق سهل الاستخدام.
- لا فرق مرئي بين الصورة الأصلية والصورة الحاملة للرسالة.
- إخفاء وجود الرسالة داخل صورة عادية.
- يعمل مع صيغ الصور الشائعة (JPEG, PNG) ويناسب الأفراد والمؤسسات.
- لا يحتاج اتصال إنترنت لاستخراج الرسالة؛ يعمل بالكامل محلياً.
- واجهة بسيطة بخطوتين فقط: اختر الصورة، ثم استخرج الرسالة.

آلية عمل StegoVault

- يستخدم خوارزمية LSB لإخفاء بيانات الرسالة داخل بكسلات الصورة دون تغيير ملحوظ.
- تدمج بيانات الرسالة داخل الصورة بطريقة تجعلها تبدو طبيعية للمستخدم.
- يُنتج صورة مطابقة للأصل بصرياً، جاهزة للمشاركة عبر أي منصة.
- المستقبل يفتح التطبيق ويستخرج الرسالة الأصلية فوراً.

المشكلة

- الحاجة لإخفاء معلومات حساسة أثناء إرسالها عبر الإنترنت دون لفت الانتباه إليها.
- الرسائل الحساسة قد تُلغى الانتباه إذا كان وجودها واضحاً أثناء الإرسال.
- أدوات الإخفاء الحالية بسيطة جداً وسهلة الكشف والاختراق.
- اعتراض الرسائل الحساسة قد يعرض الصحفيين والنشطاء والمؤسسات للخطر.

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

فريق المشروع: حمد عبدالهادي المري، عبدالله حمد الحنزاب، فيصل طارق أحمد الكشادي، مشعل ضيف الله مرجان غازي الجاسم

اسم المشروع: Nexus

نبذة عن المشروع

Nexus منصة تدريبية تفاعلية تجمع بين الشرح النظري والمحاكاة العملية للهجمات السيبرانية ضمن بيئة آمنة بالكامل، لسد الفجوة بين فهم المفهوم والقدرة على تطبيقه تحت الضغط. طوّرت بلغة Python واخُتبرت للتأكد من كفاءة الأداء ودقة الوظائف، وتأخذ المتدربين عبر هجمات محاكاة، مثل DoS وDDoS وأفضل ممارسات الدفاع جنباً إلى جنب بدل تعليمها منفصلة.

المخرجات:

- دمج النظرية والتطبيق في بيئة آمنة واحدة.
- محاكاة هجمات مثل DoS وDDoS.
- تدريب على ممارسات الدفاع مقترناً بالهجوم.
- بُنيت واخُتبرت بلغة Python لضمان الدقة.

الأهداف:

- تسهيل الانتقال من النظرية إلى التطبيق.
- بناء مهارة تقنية ووعي أمني حقيقي.
- إعداد المتدربين للتعامل المسؤول والأخلاقي.

اسم المشروع: Nexus

أعضاء الفريق: سيف رفيال بن سيف، محمد نايف الحميدي، عبدالله بن بخيت المنصوري، مبارك بن عبدالرحمن الكواري

الحل

يتمثل الحل في تطوير منصة تدريبية متكاملة تجمع بين التعليم النظري والتطبيق العملي في الأمن السيبراني داخل بيئة آمنة، من خلال محاكاة تعليمية للهجمات الإلكترونية، والتوعية بأساليب التصيد، والتدريب على أفضل ممارسات الدفاع والحماية. كما تسهم المنصة في تنمية المهارات التقنية، وتعزيز الوعي الأمني، وإعداد المتدربين للتعامل مع التهديدات السيبرانية بمسؤولية واحترافية.

المنهجية

اعتمدت منهجية المشروع على مراحل متسلسلة بدأت بتحليل المشكلة وتحديد احتياجات المتدربين، ثم تصميم نظام يدمج بين التعليم النظري والتطبيق العملي. بعد ذلك تم تطوير الاداة باستخدام لغة Python، واختبارها داخل بيئة آمنة للتأكد من كفاءة الاداء وبقية الوظائف. وفي النهاية تم تقييم النتائج وإجراء التحسينات اللازمة لضمان تحقيق الأهداف التعليمية وتقديم تجربة تدريبية متكاملة في مجال الأمن السيبراني.

التحدي

يشهد العالم تطوراً متسارعاً في التقنيات الرقمية، مما أدى إلى زيادة التهديدات السيبرانية. ويواجه المتدربون صعوبة في الانتقال من الجانب النظري إلى التطبيق العملي بسبب محدودية البيئات التدريبية التفاعلية. كما أن الفصل بين التعلم والتطبيق يقلل من فهم آليات الهجوم والدفاع بشكل متكامل. لذلك تبرز الحاجة إلى منصة تعليمية تجمع بين الشرح النظري، والمحاكاة العملية، والتدريب التفاعلي داخل بيئة آمنة، لتنمية المهارات التقنية، وتعزيز الوعي الأمني، وإعداد المتدربين للتعامل مع التهديدات السيبرانية بصورة مسؤولة وأخلاقية.

The diagram shows a flow from 'Challenge' to 'Solution' and 'Methodology'. It includes icons for a lightbulb (solution), a target (challenge), and a Python logo (methodology). Below the text, there are three small diagrams: a DoS attack diagram showing a single server being overwhelmed, a DDoS attack diagram showing multiple servers attacking a single server, and a diagram showing a network of servers connected to a central server.

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

فريق المشروع: سيف رفيال بن سيف، محمد نايف محمد الحميدي، عبدالله بن بخيت المنصوري، مبارك بن عبدالرحمن الكواري

اسم المشروع: محاكي هجمات الفدية

نبذة عن المشروع

محاكي هجمات الفدية (RansomLab) منصة تدريبية تحاكي سلوك برمجيات الفدية ضمن بيئة معزولة آمنة تماماً , "افهم العدو لتحمي نفسك" , وتعلّم المستخدمين كيفية اكتشافها والدفاع عنها دون تعريض أي نظام حقيقي للخطر. بُنيت بلغة Python في وضع تعليمي دون تشفير فعلي, وتحاكي مراحل الهجوم من الاستطلاع إلى الوصول الأولي عبر التصيد, مع تحديات متدرّجة ونظام تلميحات وتقييم مستوحى من TryHackMe.

المخرجات:

- بيئة معزولة تحاكي سلوك الفدية بأمان.
- Python بوضع تعليمي دون تشفير فعلي.
- محاكاة مراحل: استطلاع ثم وصول أولي بالتصيد.
- تحديات متدرّجة بنظام تلميحات وتقييم.

الأهداف:

- التصدي لتزايد هجمات برمجيات الفدية.
- سد الفجوة في منصات المحاكاة الآمنة.
- تمكين التعلّم دون تعريض أنظمة حقيقية للخطر.

اسم المشروع: محاكي هجمات الفدية

أعضاء الفريق: احمد فخرو , حسين السادة , عبدالله الهيدوس, علي المالكي

الحل

- توفير بيئة محاكاة آمنة: برمجيات تحاكي سلوك الفدية لأغراض التدريب دون التسبب في ضرر حقيقي.
- **تصميم المنصة:** تحديد المسارات التعليمية (كيف يبدأ الهجوم, كيف ينتشر, وكيف يتم الدفاع).



المنهجية

- دراسة عمل هجمات فدية (ransomware)
- تصميم مشهد تحاكي الهجوم في عالم آمن
- تحسين منصات من الويب تفاعلية مستوحاة من (try hack me)
- انشاء تحديات متدرّجة مع نظام تلميحات وتقييم



التحدي

- تزايد هجمات برمجيات الفدية (ransomware) على الافراد والمؤسسات
- هناك قليل من المنصات التعليمية و الامنه الذي تدربك على تحاكي الهجمات الواقعية
- هناك اشخاص لا يعرفون اكتساب خبرة تعليمية دون تعرض الانظمة الحقيقية للخطر





الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

فريق المشروع: علي سويد المالكي, عبدالله علي الهيدوس, احمد عبدالرحمن فخرو, حسين أحمد السادة

للتواصل مع الأكاديمية الوطنية للأمن السيبراني والاستفسار بشأن المخيم،
يرجى التواصل عبر الأرقام التالية:

مركز الاتصال 16555

 0097451045944 - 0097440466623 - 0097440466379

 academy@ncsa.gov.qa |  academy.ncsa.gov.qa

For inquiries regarding the camp, please contact the National Security Academy using the following numbers:

Call Center 16555

 0097451045944 - 0097440466623 - 0097440466379

 academy@ncsa.gov.qa |  academy.ncsa.gov.qa

PROJECT NAME: ADMINS - FIRST PLACE WINNER (13-14)

ABOUT THE PROJECT

An interactive educational platform for cybersecurity, designed for teenage students who lack access to specialized camps or schools. It follows an applied methodology through an online website that pairs each theoretical lesson with a real practical challenge in a safe web environment, allowing the student to move from theoretical retention to actually practicing cybersecurity skills, at a pace suited to their level.



GOALS:

- Provide teenage students real, hands-on training.
- Bridge the gap in the absence of camps and specialized schools.
- Turn theoretical knowledge into practical skills.



OUTCOMES:

- An educational website with interactive lessons.
- Practical challenges based on realistic scenarios.
- Self-paced learning paths suited to each level.
- A safe training environment accessible without attending specialized camps or schools.



Admins : اسم المشروع

اعضاء الفريق: Mariam Almousa, Menna Gabr, Joudy Hasanen, Aisha Al-Rabban

الحل

الحل هو إنشاء منصة تعليمية رقمية في مجال الأمن السيبراني، توفر محتوى تقاعلي وتحديات عملية، بحيث تمنح الطلاب فرصاً للتعليم والتدريب دون الحاجة إلى مخيمات أو مدارس خاصة.

The solution is to create a digital learning platform in cybersecurity that offers interactive content and practical challenges, giving students opportunities to learn

المنهجية

يعتمد المشروع على منهجية تطبيقية من خلال تطوير موقع الكتروني يقدم تحديثات في الأمن السيبراني، بهدف مساعدة الطلاب والمهتمين على ممارسة المعارف النظرية في بيئة واقعية آمنة باستخدام تقنيات ويب حديثة.

The project follows an applied methodology by developing a web platform with cybersecurity challenges, aiming to help students and enthusiasts practice theoretical knowledge in real-world scenarios using modern web technologies.

التحدي

هناك عدد كبير من الطلاب لديهم شغف بمجال الأمن السيبراني، إلا أنهم يقترون إلى الفرص المناسبة للالتحاق بالمخيمات الصيفية أو المدارس المتخصصة في هذا المجال.

There are a large number of students who have a passion for the field of cybersecurity, but they lack the right opportunities to attend summer camps or specialized schools in this field.



المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

PROJECT TEAM: Maryam Hassan Al-Mousa, Menna Mohammed Jaber, Jawdy Sameh Hassanein, Aisha Mohammed Al-Rabban

PROJECT NAME: SANAD - SECOND PLACE WINNER (13-14)

ABOUT THE PROJECT

Sanad is a smart platform that protects children from digital blackmail, grooming, and bullying by flagging a risk the moment it happens instead of relying on generic awareness lessons that arrive too late. Its detection engine analyses messages against a database of risk keywords across five categories combined with AI context analysis, then classifies the case using a clear Safe / Suspicious / Dangerous / Critical indicator and alerts a parent instantly, with full privacy and no child data stored.



GOALS:

- Protect children from blackmail, grooming, and bullying.
- Flag a risk the moment it happens, not after the fact.
- Break a child's silence with an instant family alert.



OUTCOMES:

- Detection engine: risk keywords plus AI context analysis.
- A clear Safe / Suspicious / Dangerous / Critical indicator.
- An instant parent alert the moment risk is detected.
- An awareness game and an Arabic and English interface.

اسم المشروع: Sanad
أعضاء الفريق: صيته عامر الحميدي، ريم سحيم الجلابي، أمنا سحيم الجلابي، هصة عبدالرحمن عبدالله

الحل

- منصة ذكية تحمي الأطفال رقمياً:
- تحليل ذكي للبيانات والإستدراج والتتبع والاحتيال.
- تفسير النتيجة لا مجرد تحذير.
- مؤشر: آمن / مشبوه / خطير / حرج.
- تنبيه فوري لولي الأمر.
- لعبة تفاعلية لبناء الوعي.
- خصوصية تامة بلا تخزين.

المنهجية

1. تحديد المشكلة: استجابة لتهديد المخاطر الإلكترونية.
2. قاعدة البيانات: طمأنينة خاطئة في 5 فئات.
3. محرك الكشف: كلمات + تحليل السياق بالذكاء الاصطناعي.
4. بناء المنصة: واجهة عميقة وإستراتيجية واقعة تفاعلية.
5. التنبيه: تحذير فوري لولي الأمر.
6. التقييم: قياس الأثر باستخدام...

التحدي

1. تعرّض الأطفال يومياً للاختراق والتتبع والاحتيال الإلكتروني.
2. ضعف الوعي الرقمي بعلامات الخطر وطرق التصرف الصحيح.
3. الطفل لا يميز المخطر إلا بعد وقوع الضرر.
4. أدوات التوعية التقليدية تلقين، ولا ترصد الخطر لحظة حدوثه.
5. الطفل يصمت خوفاً، فيعلم ولي الأمر متأخراً.

الأثر:
سند
SANAD
رقابتك للسلطة العربية
رقابتك للسلطة العربية

**المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026**

**الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy**

PROJECT TEAM: Saitah Amer Al-Hamidi, Reem Suhaim Al-Jallabi, Amna Suhaim Al-Jallabi, Hessa Abdulrahman Abdullah

PROJECT NAME: CONQUEST- THIRD PLACE WINNER (13-14)

ABOUT THE PROJECT

Conquest is a free educational website that helps beginners master Kali Linux tools without being overwhelmed by the number of options. It organizes tools into two specialized teams (Red and Blue Team) with clear use cases, pairing each tool with a ready-to-run command and a plain-language explanation of when and why to use it, covering tools such as Nmap, Hydra, Gobuster, John the Ripper, and Burp Suite.



GOALS:

- Make Kali Linux commands easier for beginners to recall.
- Clarify when and how each tool should be used.
- Provide practical learning that is completely free.



OUTCOMES:

- A website with 14 tools and 42 ready commands.
- Tools organized into three teams (Red and Blue).
- Ready commands: Nmap, Hydra, Gobuster, John the Ripper.
- Plain-language guidance on when to use each tool.

اسم المشروع: **Conquest**

أعضاء الفريق: عبدالله حمد السفران، سلطان سالم السفران، علي سالم النعيمي

ما هو منهجنا؟

Conquest هو منهج يجعل البرمجة أسهل وأكثر كفاءة. ويتميز بما يلي:

- يحتوي على 14 أداة.
- يعتمد على 3 فرق عمل بتخصصات مختلفة.
- يضم 42 أمراً جاهزاً لتسهيل العمل.
- التعلم مجاني بالكامل (0 تكلفة).

المنهجية

1. بدء المستخدم: يبدأ الطالب بتصفح الموقع Conquest مع
2. فتح برنامج Conquest: يتم تحميل البرنامج على نظام التشغيل
3. اختيار أداة: يختار الطالب أداة من بين 14 أداة (Red Team أو Blue Team)
4. يقرأ البرنامج التعليمي: يتم عرض البرنامج التعليمي الخاص بالأداة على الشاشة
5. شرح بسيط: يتم شرح الأداة بطريقة بسيطة وسهلة الفهم
6. يادرس الطالب: يادرس الطالب الأداة على جهازه الشخصي

التحدي

يواجه الطلاب المبتدئون في الأمن السيبراني صعوبة في:

- حفظ أوامر أدوات Kali Linux.
- معرفة متى وكيف يتم استخدام كل أداة.
- التنقل بين عدد كبير من الأدوات والمراجع.
- التعلم بطريقة عملية وسهلة.

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

PROJECT TEAM: Abdullah Hamad Al-Sufuran, Sultan Salem Al-Sufuran, Ali Salem Al-Naimi

PROJECT NAME: BLACK HATS - FIRST PLACE WINNER (15-17)

ABOUT THE PROJECT

Black Hats demonstrates how dangerous malware is and how hard it is to detect, in a fully safe and controlled way. The team built working simulations in Python of common malware types, namely Ransomware, a Remote Access Trojan, and a Keylogger, strictly for educational purposes, using kimi AI to identify malware behaviour and DeepSeek AI to understand the code, then drew out practical habits that reduce the chance of infection.



GOALS:

- Show how dangerous and hard to detect malware is.
- Build safe simulations for educational purposes only.
- Teach practical habits that reduce infection risk.



OUTCOMES:

- Python simulations of common malware types.
- Working models: Ransomware, RAT, and Keylogger.
- Code analysis supported by kimi AI and DeepSeek AI.
- Guidance on updates, backups, and trusted protection.

اسم المشروع: Black Hats

أعضاء الفريق: فهد الخاطر، أحمد فضل الله، علي الذواوي، عبد الله المحمود

الحل

لحماية أجهزةنا من البرمجيات الضارة، يجب:

- تحديث نظام التشغيل والبرامج باستمرار لسد الثغرات الأمنية التي قد يستغلها المهاجمون
- استخدام برامج حماية موثوقة
- إنشاء نسخ احتياطية منتظمة للملفات المهمة
- عدم فتح الروابط الممنوعة أو مجهولة المصدر
- عدم استخدام أجهزة USB أو External drive غير آمنة



المنهجية

يتبع المشروع منهجية منظمة تضمن إجراء محاكاة آمنة مع تحقيق الأهداف التوعوية في بيئة معزولة وآمنة.

استخدمنا kimi AI لتحديد لبناء البرمجيات الخبيثة. كما استخدمنا Deepseek AI لمساعدتنا في فهم الـ code بشكل أفضل.



تم كتابة الملف بلغة python حيث يحتوي على برامج خبيثة وهي:

- Ransomware
- Remote Access Trojan
- Keylogger

التحدي

مع تزايد استخدام التقنية في حياتنا اليومية، لا يزال وعي الكثير من أفراد المجتمع بمخاطر البرمجيات الخبيثة محدوداً. لا يدرك الكثيرون أن البرمجيات الخبيثة قد تُعرض بياناتهم وخصوصيتهم للخطر في لحظات، مما يجعل التوعية ضرورة لا خياراً. هدف مشروعنا هو التوعية بمدى خطورة هذه البرمجيات وصعوبة الكشف عنها عند الإصابة بها.





الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

PROJECT TEAM: Ali Abdullah Al-Dhawadi, Fahad Abdullah Al-Khater, Abdullah Jassim Al-Mahmoud, Ahmed Fadlallah Awad

PROJECT NAME: CYBERDERAA - SECOND PLACE WINNER (15-17)

ABOUT THE PROJECT

Cyberderaa brings fake-image detection and suspicious link and text checking into one place, paired with an interactive cyber assistant that raises everyday user awareness. It is built as a Python/Flask web application connected to specialized APIs: Hive Moderation for detecting fake images, VirusTotal for scanning links, and Gemini AI for analysing text, so users can verify quickly and accurately what is safe to click.



GOALS:

- Counter the rapid rise in digital fraud.
- Detect AI-generated fake images accurately.
- Make verifying links and texts fast and simple.



OUTCOMES:

- One unified scan for images, links, and text.
- A Python/Flask web app connected to security APIs.
- Hive Moderation, VirusTotal, and Gemini AI integrated.
- A cyber assistant that flags suspicious messages.

اسم المشروع: Cyberderaa

أعضاء الفريق: ملاك راشد، الهام الهاشمي، موزة جبر، الدانة منصور

الحل

فحص فوري موحد للصور والروابط والنصوص، مع مساعد سيبراني تفاعلي لتوعية المستخدمين وتحليل الرسائل المشبوهة



المنهجية

تطبيق ويب (Python/Flask) مرتبط بـ APIs للتفحص:

- Hive Moderation: لكشف الصور المزيفة.
- VirusTotal: لفحص الروابط.
- Gemini AI: لتحليل النصوص



التحدي

- تزايد الاحتيال
- تزايد الصور المزيفة المولدة بالذكاء الاصطناعي.
- صعوبة التحقق من سلامة الروابط والنصوص





المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

PROJECT TEAM: Al-Dana Mansour Salem Al-Naimi, Moza Jaber Mohammed Jassim Al-Thani, Malak Rashed Fahad Al-Dosari, Elham Abdul Majeed Al-Hashemi

ABOUT THE PROJECT

Operation Shadow is an interactive simulation that puts the user in the role of a security analyst facing a full escalating attack, from phishing through to data theft. Every decision, right or wrong, actually changes the attack path and its outcome, supported by a live network map, a smart assistant (SHADOW AI), and a final assessment that shows performance. It is an easy-to-use web platform that runs in the browser without internet and scales to institutions.



GOALS:

- Show human error as the main cause of breaches.
- Replace theoretical awareness with real experience.
- Enable real decision-making during an attack.



OUTCOMES:

- A full simulation from phishing to data theft.
- User decisions actively change the attack path.
- A live network map and the SHADOW AI assistant.
- A scalable web platform that runs without internet.

اسم المشروع: Operation Shadow
أعضاء الفريق: لطيفة الحنزاب، نجود المالكي، عايشة المري

الحل	المنهجية	التحدي
• منصة "عملية الظل" تحول التوعية الأمنية من محتوى نظري إلى تجربة تفاعلية تحاكي الهجمات السيبرانية. • تمكن المستخدم من التعلم بالممارسة ورؤية تأثير قراراته مباشرة، مع تقييم يوضح نقاط القوة والضعف. • منصة سهلة الاستخدام، تعمل عبر المتصفح وبدون اتصال بالإنترنت، وقابلة للتوسعة لتناسب المدارس والجامعات والشركات.	• تطوير محاكاة تفاعلية لهجوم سيبراني متكامل تبدأ بالتصيد الاحتيالي وتنتهي بمحاولة سرقة البيانات. • إشراك المستخدم في دور محلل أمني لاتخاذ قرارات تؤثر مباشرة على سير الهجوم ونتائجه. • دعم التجربة بخريطة شبكة حيّة، ومساعد ذكي (SHADOW AI)، وتقييم نهائي يوضح الأداء وتأثير القرارات.	• تزايد الهجمات السيبرانية، ويُعد الخطأ البشري السبب الرئيسي لنجاح معظم الاختراقات. • تعتمد برامج التوعية الحالية على أساليب نظرية لا تُعدّ الموظفين للتعامل مع الهجمات الفعلية. • غياب حلول تدريبية تفاعلية وأمنة تمنح المستخدم تجربة واقعية لاتخاذ القرارات أثناء الهجوم.

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

PROJECT TEAM: Al-Dana Mansour Salem Al-Naimi, Moza Jaber Mohammed Jassim Al-Thani, Malak Rashed Fahad Al-Dosari, Elham Abdul Majeed Al-Hashemi

PROJECT NAME: CASE FILES

ABOUT THE PROJECT

Case Files is an interactive cybersecurity game that turns learning into a live digital forensic investigation. Students take on the role of a cyber investigator handed a real breach case: they collect digital evidence, analyse clues, and complete capture-the-flag (CTF) challenges to uncover exactly how the attacker got in, then build a prevention plan and earn a completion certificate, living the consequences of security decisions instead of memorizing facts.



GOALS:

- Raise awareness of phishing and weak passwords.
- Replace rote learning with hands-on practice.
- Train digital investigation and evidence analysis.



OUTCOMES:

- An investigation journey: case, evidence, CTF challenges.
- Every player builds a prevention plan before closing.
- A scoring system with a digital completion certificate.
- Simulated threats: phishing and weak passwords.

اسم المشروع: Sanad

أعضاء الفريق: صيته عامر الحميدي، ريم سحيم الجلابي، آمنه سحيم الجلابي، حصه عبدالرحمن عبدالله

الهدف

- منصة ذكية تحمي الأطفال رقمياً:
- تحليل ذكي للابتزاز والاستدراج والتتبع والاحتيال.
- تفسير النتيجة لا مجرد تحذير.
- مؤشر: أمن / مشبوه / خطير / حرج.
- تنبيه فوري لولي الأمر.
- لعبة تفاعلية لبناء الوعي.
- خصوصية تامة بلا تخزين.

سناد
SANAD
والتحديات للوعي الرقمي
Your Companion for Digital Safety

الأثر:
جيل واع
وأُسرة شريكة

المنهجية

- 1 تحديد المشكلة
أسئلة الفهم المحاور والوعي.
- 2 قاعدة البيانات
خدمات خطرة في 0 فئات
- 3 محرك الكشف
كلمات + تحليل السياق بالكلمات البديلة
- 4 بناء المنصة
واجهة عربية واجهته ومناهج تفاعلية
- 5 التنبيه
تحذير فوري لولي الأمر
- 6 التقييم
قياس أثر المنصة

التحدي

1. تعرض الأطفال يومياً للابتزاز والاستدراج والتتبع والاحتيال الإلكتروني.
2. ضعف الوعي الرقمي بعلامات الخطر وطرق التصرف الصحيح.
3. الطفل لا يميز المحتال إلا بعد وقوع الضرر.
4. أدوات التوعية التقليدية ثقيلة، ولا ترصد الخطر لحظة حدوثه.
5. الطفل يصمت خوفاً فيعلم ولي الأمر متأخراً.

أ. عدد حالات خطرة على الأطفال في بيئة رقمية (معدل شهري)

البيئة	الخطورة
البيئة	100%
البيئة	80%
البيئة	60%
البيئة	40%

ب. عدد حالات خطرة على الأطفال في بيئة رقمية (معدل شهري)

البيئة	الخطورة
البيئة	100%
البيئة	80%
البيئة	60%
البيئة	40%

ج. عدد حالات خطرة على الأطفال في بيئة رقمية (معدل شهري)

البيئة	الخطورة
البيئة	100%
البيئة	80%
البيئة	60%
البيئة	40%

المكيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

PROJECT TEAM: Fatima Al-Ansari, Shahad Mohsen, Naeema Mohammed Al-Bahli, Al-Jazi Al-Kuwari

PROJECT NAME: CYBERDREAMS

ABOUT THE PROJECT

Cyberdreams is a comprehensive platform that uses AI to analyse links, emails, and QR codes at once, rating the risk of each with clear, actionable protection advice. It brings six separate tools, a phishing analyzer, a QR analyzer, an email analyzer, a website privacy analyzer, a learning hub, and a password generator, into a single dashboard, so users no longer switch between apps, and every analysis result is saved for later review.



GOALS:

- Counter the growing spread of phishing attacks.
- Simplify verifying suspicious links and messages.
- Raise security awareness with easy-to-use tools.



OUTCOMES:

- AI analysis of links, messages, and QR codes.
- Six integrated tools in a single dashboard.
- Phishing, QR, email, and site-privacy analyzers.
- Instant reports with a saved analysis history.

اسم المشروع: Cyberdreams
أعضاء الفريق: الجوري العتيبي، المها الهيال، هيا العبدالله

الحل	المنهجية	التحدي
١- محلل روابط التصيد الإحتيالي	يقوم المستخدم بإدخال رابط أو رسالة بريد إلكتروني أو رمز (QR) أو سؤال.	١- إنتشار هجمات التصيد الإلكتروني (phishing)
٢- محلل رموز الاستجابة السريعة (QR)	قوم النظام بتحليل البيانات باستخدام الذكاء الاصطناعي.	٢- صعوبة التحقق من الروابط و رسائل البريد الإلكتروني المشبوهة
٣- محلل البريد الإلكتروني	يحدد مستوى الخطورة.	٣- نقص الوعي الأمني لدى المستخدمين
٤- محلل خصوصية المواقع الإلكترونية	يقدم تقريرًا ونصائح لحماية المستخدم.	
٥- مركز التعلم	يحفظ نتائج التحليل لعرضها لاحقًا.	
٦- مولد كلمات المرور		

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

PROJECT TEAM: Al-Jouri Abdulaziz Al-Otaibi, Al-Maha Khaled Al-Hayal, Haya Jaithan Al-Abdullah

PROJECT NAME: HEXAGUARD

ABOUT THE PROJECT

HexaGuard is a defensive system that automatically monitors connected USB devices and analyses their files before the user opens anything. Instead of guessing, it generates a SHA-256 digital fingerprint for every file, compares it against the VirusTotal threat database, then calculates a clear risk score using a multi-technique detection engine and displays an actionable recommendation, with every result saved to a Scan History log.



GOALS:

- Assess the risk of USB files before opening them.
- Automate scanning instead of relying on guesswork.
- Give a clear, practical security recommendation.



OUTCOMES:

- Automatic USB detection and file scanning.
- A SHA-256 fingerprint for every file before opening.
- VirusTotal comparison with a calculated risk score.
- A Scan History log of results and recommendations.

اسم المشروع: HexaGuard

أعضاء الفريق: رايه عبدالله المهندي، دانة عبدالقادر بابكر، أمل فاطمة

الحل



HexaGuard هو نظام دفاعي يقوم بمراقبة أجهزة التخزين القابلة للإزالة وتحليل الملفات الموجودة عليها باستخدام تقنيات متعددة، ثم يعرض تقريراً يوضح مستوى الخطورة ويوفر توصيات تساعد المستخدم على اتخاذ القرار المناسب.

المنهجية

- اكتشاف جهاز USB المتصل.
- فحص الملفات الموجودة على الجهاز.
- إنشاء بصمة رقمية (SHA-256) لكل ملف.
- مقارنة البصمة مع قاعدة بيانات VirusTotal.
- حساب درجة الخطورة باستخدام محرك تقييم المخاطر.
- عرض تقرير ورسالة توصية للمستخدم.
- حفظ نتائج الفحص في سجل Scan History.



التحدي

تعد أجهزة التخزين القابلة للإزالة مثل وحدات USB وسيلة شائعة لنقل الملفات، لكنها قد تشكل خطراً أمنياً بسبب إمكانية احتوائها على ملفات ضارة أو غير موثوقة. يحتاج المستخدم إلى وسيلة تساعد على تقييم مستوى خطورة هذه الملفات قبل استخدامها.



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

PROJECT TEAM: Raya Abdullah Al-Mohannadi, Dana Abdul Qader Babiker, Amal Fatima

PROJECT NAME: QSECURE

ABOUT THE PROJECT

QSecure is a smart honeypot platform (QAHN) that runs inside an organization's network and constantly changes its identity using quantum random number generation (QRNG), making it far harder to detect or predict than traditional decoys. An adaptation engine continuously reshapes the operating system fingerprint, login pages, open ports, and decoy files, and the system automatically resets its configuration whenever suspicious activity is detected.



GOALS:

- Address how easily static honeypots are detected.
- Build a smarter, more adaptive decoy system.
- Increase the unpredictability of honeypot characteristics.



OUTCOMES:

- A QAHN honeypot platform inside the network.
- QRNG continuously reshapes the honeypot identity.
- Changing ports, login pages, and decoy files.
- Automatic reset when suspicious activity is detected.

اسم المشروع: Qsecure

أعضاء الفريق: عائشة طارق الخاطر، شهد محمد قاسم، فجر علي العمادي

الحل

- تغيير هوية الخادم باستمرار.
- منافذ وخدمات ديناميكية.
- صفحات تسجيل دخول متنوعة.
- ملفات وهمية تتغير باستمرار.
- استخدام QRNG لزيادة عدم قابلية التنبؤ.



المنهجية

- منصة برمجية متخصصة QAHN تعمل داخل شبكة المؤسسة لحماية أنظمتها من الهجمات الإلكترونية.
- توليد أرقام عشوائية باستخدام موك الأرقام العشوائية الكمية (QRNG).
- إرسال القيم إلى محرك التكيف.
- تغيير خصائص المعصيدة بشكل مستمر، مثل:
 - نظام التشغيل.
 - صفحة تسجيل الدخول.
 - المنافذ المفتوحة.
 - الملفات والخدمات الوهمية.
 - عند اكتشاف نشاط مشبوه يعيد النظام تغيير إعداداته تلقائياً لإرباك المهاجم.



التحدي

- يستطيع المهاجمون اكتشاف (HoneyPot) من خلال تحليل المنافذ المفتوحة، ونظام التشغيل، وسلوك الخادم.
- عند اكتشافها، يتوقف المهاجم عن التفاعل معها، مما يقلل من المعلومات التي يحصل عليها قريب.
- مع تطور الهجمات الإلكترونية، أصبحت الحاجة إلى مصائد أكثر نكاهاً وتكيفاً ضرورية.



المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

PROJECT TEAM: Aisha Tarek Al-Khater, Shahad Mohammed Qassem, Fajer Ali Al-Emadi

PROJECT NAME: HSN PLATFORM

ABOUT THE PROJECT

Hisn is a unified platform that uses AI to scan links, messages, QR codes, images, and privacy policies and rate their risk in one place, instead of forcing users to switch between a separate tool for every threat. It analyses content using AI models and trusted databases to identify the threat type and level, shows a safe preview of links, and summarizes privacy policies in plain language, with a smart assistant and an emergency mode for immediate response.



GOALS:

- Bring scattered protection tools into one platform.
- Speed up response instead of splitting attention.
- Enable users to make the right decision before any interaction.



OUTCOMES:

- One unified scan: links, messages, QR codes, images.
- Safe link preview and fake-image detection.
- Privacy policies summarized in plain language.
- A smart assistant and an emergency response mode.

اسم المشروع: حصن

أعضاء الفريق: فاطمة جعفري، حصة التميمي، وضحة المري، ليلي أشكاناني، فاطمة المالكي

الحل

منصة حصن الذكية توفر للمستخدم مجموعة من أدوات الحماية في مكان في مكان واحد، وتشمل:

- فحص الروابط مع عرض معاينة آمنة لمحتواها
- فحص رموز QR واكتشاف الروابط الضارة قبل فتحها
- تحليل الرسائل النصية للكشف عن رسائل التصيد والاحتيال
- التحقق من أصالة المحتوى وكشف الصور المزيفة
- حماية خصوصية الصور عبر إزالة البيانات الخفية
- تحليل وتخصيص سياسات الخصوصية للمواقع بلغة مبسطة
- مساعد ذكي يقدم إرشادات ونوعية أمنية فورية
- الإبلاغ عن عمليات الاحتيال لدعم رفع الوعي
- وضع الطوارئ الذي يوفر إرشادات فورية وخطوات الاستجابة عند الاشتباه بالتعرض لهجوم أو اختراق

المنهجية

تم تطوير منصة حصن بالاعتماد على منهجية تجمع بين تقنيات الذكاء الاصطناعي وأدوات تحليل الأمن السيبراني في منصة موحدة

- تستقبل المنصة منخلات المستخدم: (روابط، رسائل، QR، صور، سياسات الخصوصية)
- يتم تحليل المحتوى باستخدام نموذج ذكاء اصطناعي وقواعد بيانات آمنة موثوقة وأدوات متقدمة
- يتم تقييم مستوى الخطورة وتحديد نوع التهديد واحتمالية
- تقديم نتائج فورية مدعومة بتوصيات واضحة وإرشادات عملية لحماية المستخدم
- تمكين المستخدم من اتخاذ القرار الصحيح قبل التفاعل مع أي محتوى رقمي

التحدي

مع التطور المتسارع للهجمات السيبرانية، أصبح المستخدم يواجه تهديدات متنوعة مثل:

- روابط التصيد والاحتيال
- رموز QR الخبيثة
- الرسائل الاحتمالية والهندسة الاجتماعية
- الصور المزيفة والمحتوى المزيف
- سياسات الخصوصية المعقدة
- الحاجة لاستخدام أدوات متعددة ومتفرقة للتحقق من كل تهديد

النتيجة:

هذا التثشت يقلل من سرعة الاستجابة ويؤيد من احتمالية الوقوع ضحية للهجمات الإلكترونية

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

PROJECT TEAM: Fatima Issa Shaaban Jaafari, Hessa Mansour Al-Naimi, Wadha Mohammed Rashed Al-Marri, Laila Ashkanani, Fatima Hussein Al-Malki

PROJECT NAME: GAS FORTRESS

ABOUT THE PROJECT

Gas Fortress is an AI-powered website that protects gas sector employee data from leaking during crises and geopolitical risk, when reliance on external AI tools such as Copilot, which process data through external clouds, is at its peak. The system checks every message or file against a whitelist and analyses its content, then either blocks sensitive material instantly or forwards the request while recording its risk level and the reason, protecting strategic secrets and production figures.



GOALS:

- Reduce reliance on external clouds for data.
- Protect strategic secrets and production data.
- Strengthen cybersecurity during crisis periods.



OUTCOMES:

- An AI-powered site protecting employee data.
- Inputs checked against a whitelist before sending.
- Instant blocking of sensitive data during risk periods.
- A recorded risk level and reason for every request.



PROJECT TEAM: Rahaf Saleh Al-Marri, Fajer Hamad Al-Kuwari, Nora Saleh Al-Marri

PROJECT NAME: CYBER FALCONS

ABOUT THE PROJECT

Cyber Falcons is an integrated platform that brings several previously separate security tools into one place for malware analysis and link scanning. It supports different file types and lets users test how long their own passwords would realistically take to crack, along with a phishing awareness test, educational content, and videos from international sources. It was built through structured phases: requirements analysis, design, development, testing, then deployment and evaluation.



GOALS:

- Merge several security tools into one platform.
- Improve performance so the project runs smoothly.
- Integrate project components and handle errors.



OUTCOMES:

- An integrated platform for malware and link analysis.
- Support for analysing different file types.
- Password-cracking time and phishing awareness tests.
- Educational content and videos from global sources.



PROJECT TEAM: Saleh Rashed Al-Adhba, Fahad Musfer Al-Marri, Sultan Fahad Al-Mohannadi, Mohsen Nayef Al-Shammari

PROJECT NAME: FILESHIELD

ABOUT THE PROJECT

FileShield continuously monitors sensitive files and detects any unauthorized change the moment it happens, using a SHA-256 digital fingerprint signed with a passphrase. Instead of discovering a breach months later through a slow manual check, the user gets an instant alert for four events: modification, copying, deletion, or renaming. It was built in JavaScript/React using Claude and VSCode, with a live dashboard in Arabic and English.



GOALS:

- Detect file changes immediately, not months later.
- Replace manual checking with automated monitoring.
- Guarantee and verify the integrity of sensitive files.



OUTCOMES:

- Instant detection of four types of file change.
- A SHA-256 fingerprint signed with a passphrase.
- A live monitoring dashboard in Arabic and English.
- Built in JavaScript/React using Claude and VSCode.

اسم المشروع: FileShield

أعضاء الفريق: يوسف احمد عبيدالله، محمد سلمان العامري، علي سالم المري

الحل

- الكشف الفوري لأربع حالات
- بصمة SHA-256 موقعة بعبارة مرور
- مراقبة حية بلغة عربية وإنجليزي



المنهجية

- استخدمنا كلاود مع Vscod
- استخدمنا لغة البرمجة / Javascript react
- اعتمدنا بصمة SHA-256 مرجعا للمقارنة

التحدي

- ملفات حساسة تعدل دون أن يلاحظ أحد
- الاكتشاف يأتي بعد أشهر من الضرر
- الفحص اليدوي للملفات مستحيل



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

PROJECT TEAM: Yousef Ahmed Obaidullah, Mohammed Salman Al-Amri, Ali Salem Saleh Al-Sufran Al-Marri

PROJECT NAME: HOMAND

ABOUT THE PROJECT

HOMAND is a unified platform that searches for a user's scattered digital identity across roughly 65 platforms at once, running 18 professional security tools in parallel with AI-backed verification of results as they arrive. Instead of manually checking dozens of sites for hours and still missing exposed accounts, the user gets a live, readable report within minutes, for authorized educational use only.



GOALS:

- Unify identity searching across dozens of platforms.
- Replace manual checking with AI-backed scanning.
- Bring complex security tools into one simple platform.



OUTCOMES:

- Automated search across roughly 65 platforms.
- 18 professional security tools running in parallel.
- AI-backed verification with live results.
- Saved, readable reports produced within minutes.

اسم المشروع: HOMAND
أعضاء الفريق: حسن ماجد العلي، سالم محمد المري، خالد سامي الياقفي، عبد العزيز عبد الله السليطي

الحل

- منصة ويب واحدة سهلة
- بحث عن الهوية + ذكاء اصطناعي
- 18 أداة أمنية احترافية
- استخدام تعليمي مصرح به فقط



المنهجية

- البحث في 65 منصة دفعة واحدة
- تأكيد الهوية بالذكاء الاصطناعي
- تشغيل 18 أداة أمنية بتوازي
- نتائج حية وتقارير محفوظة



التحدي

- حسابات الشخص مبعثرة على منصات كثيرة
- أدوات منفصلة ومعقدة
- تأكيد الهوية يدوي ويستغرق ساعات
- لا توجد منصة موحدة





الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

PROJECT TEAM: Hassan Majed Al-Ali, Salem Mohammed Al-Marri, Khaled Sami Al-Yafei, Abdulaziz Abdullah Al-Sulaiti

PROJECT NAME: IRSHAAD

ABOUT THE PROJECT

IRSHAAD is an interactive awareness platform built to spread real cybersecurity culture among children and adults through simplified lessons, practical tools, and interactive quizzes rather than dense technical material. It includes an interactive toolkit of around 30 tools, a live threat map, an email breach checker, and a phishing lab, with a built-in AI assistant that answers questions instantly and an internal scoring system that tracks each user's progress over time.



GOALS:

- Raise awareness of phishing and fraud at all ages.
- Design content suited to different age groups.
- Provide instant AI help during the learning process.



OUTCOMES:

- A platform with lessons, tools, and interactive quizzes.
- Around 30 tools: link, password, and hash analysis.
- A live threat map and an email breach checker.
- An AI assistant and a progress tracking system.

اسم المشروع: IRSHAAD

أعضاء الفريق: حمد أحمد المحشادي، سيف علي سعيد
البريص، محمد سالم المحمد، خالد محمد الرشدي

الحل

IRSHAAD Cybersecurity Awareness

هي منصة تعليمية تفاعلية تهدف إلى نشر ثقافة الأمن السيبراني لدى الأطفال والكبار، من خلال دروس مبسطة، أدوات عملية، واختبارات تفاعلية تساعد المستخدم على اكتساب مهارات الحماية الرقمية بطريقة ممتعة وسهلة.



المنهجية

- 1 دراسة أكثر التهديدات السيبرانية انتشاراً.
- 2 تصميم محتوى تعليمي يناسب مختلف الفئات العمرية.
- 3 تطوير منصة تفاعلية تضم أدوات تعليمية واختبارات.
- 4 دمج تقنيات الذكاء الاصطناعي لتقديم المساعدة الفورية.
- 5 تقييم أداء المستخدم وقياس تقدمه من خلال التحديات والأنشطة.

التحدي

مع تزايد استخدام الإنترنت، يواجه الأطفال والكبار مخاطر سيبرانية مثل التصيد الإلكتروني وسرقة الحسابات والاحتيال الرقمي، مما يستدعي تعزيز الوعي بالأمن السيبراني عبر وسائل تعليمية تفاعلية وسهلة الاستخدام.



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

PROJECT TEAM: Hamad Ahmed Al-Mahashadi, Saif Ali Saeed Al-Breis, Mohammed Salem Al-Mohammed, Khaled Mohammed Al-Rashidi

PROJECT NAME: PHISH GUARD AI

ABOUT THE PROJECT

Phish Guard AI uses artificial intelligence to analyse suspicious messages, emails, and images and determine how likely they are to be phishing, with a clear explanation of why. Instead of relying on appearance alone, it extracts text from images using OCR, checks for suspicious word patterns such as Urgent, Verify, and Free, and inspects embedded links for known fake domains, then assigns a risk score from 0 to 100, alongside an educational game, Phishing or Not.



GOALS:

- Counter the widespread rise of phishing attacks.
- Make fake messages reliably easy to identify.
- Raise awareness of email and image-based attacks.



OUTCOMES:

- A risk score from 0 to 100 with an explanation.
- Text extracted from images using OCR.
- Checks for suspicious word patterns and links.
- The Phishing or Not game and Battle Mode.

اسم المشروع: Phish Guard Team
أعضاء الفريق: مشعل المفتاح , علي الفضالة

الحل

منصة Phish Guard AI
تحليل الرسائل والإيميلات والصور
تحديد مستوى الخطورة (أمن / خطر / مشبوه)
شرح سبب التصنيف للمستخدم لتقديم
نصائح للحماية
لعبة تعليمية (Phishingor Not+ BattleMode)

المنهجية

استخدام الذكاء الاصطناعي لتحليل النصوص
والصور فحص الروابط واكتشاف النطاقات المزيفة
تحليل الكلمات المشبوهة مثل (Urgent/ Verify / Free)
استخراج النص من الصور (OCR) وتحليله
إعطاء درجة خطورة من 0 إلى 100
بناء لعبة تفاعلية لزيادة الوعي

التحدي

انتشار هجمات التصيد الاحتيالي بشكل
كبير
صعوبة تمييز الرسائل المزيفة من
الحقيقية
اعتماد المستخدمين على الشكل بدل
التحقق من المصدر
زيادة الهجمات عبر البريد الرسائل والصور
ضعف الوعي بالأمن السيبراني

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

PROJECT TEAM: Meshal Saud Al-Miftah, Ali Mohammed Al-Fadala

PROJECT NAME: STEGOVAULT

ABOUT THE PROJECT

StegoVault hides sensitive messages inside ordinary-looking images using the LSB algorithm, with no visible difference between the original image and the one carrying the message, and no internet connection required. It works entirely offline, supports JPEG and PNG through a simple two-step interface (choose the image, then extract the message), and was designed for cases where sending openly would attract unwanted attention: journalists, activists, and institutions.



GOALS:

- Hide information in transit without drawing attention.
- Overcome the weakness of easily detected tools.
- Protect journalists and activists from interception.



OUTCOMES:

- Messages hidden with LSB, with no visible difference.
- Runs fully offline with no internet required.
- Supports JPEG and PNG via a two-step interface.
- A carrier image identical to the original, ready to share.

اسم المشروع: StegoVault

أعضاء الفريق: حمد عبدالهادي المري، عبدالله حمد الحنزاب، فيصل طارق أحمد الكشادي، مشعل ضيف الله مرجان غازي الجاسم

الميزات StegoVault	آلية عمل StegoVault	المشكلة
• إخفاء الرسائل في خطوة واحدة داخل تطبيق سهل الاستخدام. • لا فرق مرئي بين الصورة الأصلية والصورة الحاملة للرسالة. • إخفاء وجود الرسالة داخل صورة عادية. • يعمل مع صيغ الصور الشائعة (JPEG, PNG) ويناسب الأفراد والمؤسسات. • لا يحتاج اتصال إنترنت لاستخراج الرسالة؛ يعمل بالكامل محلياً. • واجهة بسيطة بخطوتين فقط: اختر الصورة، ثم استخرج الرسالة.	• يستخدم خوارزمية LSB لإخفاء بيانات الرسالة داخل بكسلات الصورة دون تغيير ملحوظ. • تُدمج بيانات الرسالة داخل الصورة بطريقة تجعلها تبدو طبيعية للمستخدم. • يُنتج صورة مطابقة للأصل بصرياً، جاهزة للمشاركة عبر أي منصة. • المستقبل يفتح التطبيق ويستخرج الرسالة الأصلية فوراً.	• الحاجة لإخفاء معلومات حساسة أثناء إرسالها عبر الإنترنت دون لفت الانتباه إليها. • الرسائل الحساسة قد تُلغى الانتباه إذا كان وجودها واضحاً أثناء الإرسال. • أدوات الإخفاء الحالية بسيطة جداً وسهلة الكشف والاختراق. • عقراض الرسائل الحساسة قد يعرض الصحفيين والنشطاء والمؤسسات للخطر.



المؤتمر الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

PROJECT TEAM: Hamad Abdul Hadi Al-Marri, Abdullah Hamad Al-Hinzab, Faisal Tarek Ahmed Al-Kashadi, Meshal Dhaifullah Marjan Ghazi Al-Jassim

PROJECT NAME: NEXUS

ABOUT THE PROJECT

Nexus is an interactive training platform that combines theoretical explanation with practical simulations of cyberattacks in a fully safe environment, built to close the gap between understanding a security concept and being able to apply it under pressure. It was developed in Python and carefully tested for performance and functional accuracy, taking trainees through simulated attacks such as DoS and DDoS alongside defensive best practices rather than teaching them separately.



GOALS:

- Ease the move from theory to practical application.
- Build genuine technical skill and security awareness.
- Prepare trainees to act responsibly and ethically.



OUTCOMES:

- Theory and practice combined in one safe environment.
- Simulated attacks such as DoS and DDoS.
- Defence training paired directly with attack simulation.
- Built and tested in Python to ensure accuracy.

اسم المشروع: Nexus

أعضاء الفريق: سيف رفايل بن سيف، محمد نايف الحميدي، عبدالله بن بخيت المنصوري، مبارك بن عبدالرحمن الكواري

الحل

يتمثل الحل في تطوير منصة تدريبية متكاملة تجمع بين التعليم النظري والتطبيق العملي في الأمن السيبراني داخل بيئة آمنة، من خلال محاكاة تعليمية للهجمات الإلكترونية، والتوعية بأساليب التصيد، والتدريب على أفضل ممارسات الدفاع والحماية. كما تسهم المنصة في تنمية المهارات التقنية، وتعزيز الوعي الأمني، وإعداد المتدربين للتعامل مع التهديدات السيبرانية بمسؤولية واحترافية.

المنهجية

اعتمدت منهجية المشروع على مراحل متسلسلة بدأت بتحليل المشكلة وتحديد احتياجات المتدربين، ثم تصميم نظام يدمج بين التعليم النظري والتطبيق العملي. بعد ذلك تم تطوير الأداة باستخدام لغة Python، واختبارها داخل بيئة آمنة للتأكد من كفاءة الأداء ودقة الوظائف. وفي النهاية تم تقييم النتائج وإجراء التحسينات اللازمة لضمان تحقيق الأهداف التعليمية وتقديم تجربة تدريبية متكاملة في مجال الأمن السيبراني.

التحدي

يشهد العالم تطوراً متسارعاً في التقنيات الرقمية، مما أدى إلى زيادة التهديدات السيبرانية. ويواجه المتدربون صعوبة في الانتقال من الجانب النظري إلى التطبيق العملي بسبب محدودية البيانات التدريبية التفاعلية. كما أن الفصل بين التعلم والتطبيق يقلل من فهم آليات الهجوم والدفاع بشكل متكامل. لذلك تبرز الحاجة إلى منصة تعليمية تجمع بين الشرح النظري، والمحاكاة العملية، والتدريب التفاعلي داخل بيئة آمنة، لتنمية المهارات التقنية، وتعزيز الوعي الأمني، وإعداد المتدربين للتعامل مع التهديدات السيبرانية بصورة مسؤولة وأخلاقية.

DoS attack: Target system -> Malicious traffic -> Denial of service

DDoS attack: Multiple systems -> Malicious traffic -> Denial of service

PROJECT TEAM: Saif Rafial bin Saif, Mohammed Nayef Mohammed Jaber Nasser Al-Hamidi, Abdullah bin Bukhait Al-Mansouri, Mubarak bin Abdulrahman Al-Kuwari

PROJECT NAME: RANSOMWARE ATTACK SIMULATOR

ABOUT THE PROJECT

The Ransomware Attack Simulator (Ransomware) is a training platform that mimics ransomware behaviour inside a fully isolated, safe environment, on the principle of knowing the enemy to protect yourself, teaching users how to detect and defend against it without putting any real system at risk. It was built in Python in educational mode with no actual encryption, simulating the attack stages from reconnaissance to initial access via phishing, with graded challenges, a hint system, and scoring inspired by TryHackMe.



GOALS:

- Counter the rise in ransomware attacks.
- Close the gap in safe simulation platforms.
- Enable learning without risking real systems.



OUTCOMES:

- An isolated environment that mimics ransomware safely.
- Python in educational mode with no real encryption.
- Simulated stages: reconnaissance then phishing access.
- Graded challenges with a hint and scoring system.

اسم المشروع: محاكي هجمات الفدية

أعضاء الفريق: احمد فخرو , حسين السادة , عبدالله الهيدوس, علي المالكي

الحل

- توفير بيئة محاكاة آمنة: برمجيات تحاكي سلوك الفدية لأغراض التدريب دون التسبب في ضرر حقيقي.
- **تصميم المنصة:** تحديد المسارات التعليمية (كيف يبدأ الهجوم، كيف ينتشر، وكيف يتم الدفاع).



المنهجية

- دراسة عمل هجمات فدية (ransomware)
- تصميم مشهد تحاكي الهجوم في عالم آمن
- تحسين منصات من الويب تفاعلية مستوحاة من (try hack me)
- انشاء تحديات متدرجة مع نظام تلميحات وتقييم



التحدي

- تزايد هجمات برمجيات الفدية (ransomware) على الافراد والمؤسسات
- هناك قليل من المنصات التعليمية و الامنه الذي تدربك على تحاكي الهجمات الواقعية
- هناك اشخاص لا يعرفون اكتساب خبرة تعليمية دون تعرض الانظمة الحقيقية للخطر





الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

PROJECT TEAM: Ali Suwaid Al-Malki, Abdullah Ali Al-Haidous, Ahmed Abdulrahman Fakhroo, Hussein Ahmed Al-Sadah

Graduation Projects

المخيم الشبابي لل
YOUTH CAMP 2026



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

شبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH C



TALENT ADOPTION MECHANISM



PARTICIPANTS' VIEWS ON THE CAMP



This is my third year at the Cyber Security Camp, and each year I notice a clear improvement in the quality of content and information provided. I thoroughly enjoyed my experience at the camp, and it was so positive that it encouraged my relatives to register and take part in it.

- Student Hamad Mohammed Al-Mahshadi Al-Maadheed



"This was my first time participating in the Cyber Security Camp, and I registered based on a recommendation from my relatives. I gained a lot from the information and skills I learned during the program, and it was a distinctive and enriching experience for me."

- Student Fahad Hamad Al-Marri



"What I liked most about the camp was that it combined learning with activities and games that helped us stay alert and focused, in addition to the attention given to evaluation at the end of each week."

- Student Aisha Tariq Al-Khater



"What I liked most about the camp was the organizers, who were cooperative and always available to help. I also enjoyed the diversity and fun of the activities, and how each event differed from the other, which made my experience at the camp beautiful and distinctive."

- Student Lolwa Nasser Al-Kuwari

FEEDBACK BASED ON STUDENTS' & SUPERVISORS' COMMENTS

Overall Organization and Experience

Praise for the overall level of organization and the camp experience, with suggestions to improve the scheduling of sessions, breaks, and activities.

Trainers and Administrators

Satisfaction with the cooperation of trainers and administrators and their support for participants, with appreciation for their explanation style, interaction, and follow-up.

Content and Practical Application

Clear interest in cyber security content, with a desire for more practical applications and CTF challenges and less theoretical content.

Activities and Competitions

Positive engagement with recreational and group activities, with requests to increase them and add more sports, physical activities, and inter-class competitions.

Interactive Activities

Enthusiasm for hands-on experiences, with suggestions to extend activity time and add new events.

Future Development

Participants expressed interest in new activities including sports, practical cyber challenges, group games, handicrafts, and trips.

CAMP STATISTICS



15

Core topics



1000

Online Participants



349

Participants



6

Cyber challenges



8

Visiting experts



25

Trainers



15

Days of activities



80

Graduation projects



4

Field visits



50

Hours of training



4

Partners



Honoring the Winning Teams for Best Graduation Projects

1st Place



Winning Teams:
Admins, Black Hats



Students Honored: 8
Prize: iPhone 17

2nd Place



Winning Teams:
Cyberderaa, Sanad



Students Honored: 8
Prize: iPhone 17

3rd Place



Winning Teams:
Operation Shadow, Conquest



Students Honored: 8
Prize: iPhone 17

THEATRICAL PERFORMANCE & CAMP JOURNEY VIDEO

The video presented the key stages of the students' journey through the camp, from training, practical activities, and challenges, to the development of graduation projects and participation in the closing ceremony — documenting the students' experience and the skills and knowledge they gained during the program.



Theatrical Performance: From a Passion for Gaming to National Responsibility

A collection of photos documenting the theatrical performance presented by camp students during the closing ceremony.



GRADUATION PROJECTS

During the Cybersecurity Youth Camp, students developed graduation projects covering a wide range of cybersecurity-related fields. As part of the closing ceremony, the top 20 graduation projects were given the opportunity to be showcased to parents, partners, and guests, with participation from both age groups (13–14 and 15–17 years old).

The projects covered several areas of cybersecurity, including network security, ethical hacking, cyber defense, and web application security. They demonstrated the level of practical knowledge and skills that students acquired and developed throughout the three-week camp.

The exhibition also provided a platform for students to present their ideas and showcase the practical outcomes of the camp, highlighting its impact on developing participants' cybersecurity skills.

- 80 graduation projects covering various fields of cybersecurity.
- 20 graduation projects qualified for the finals.
- Two age groups: 13-14 and 15-17 years.
- 4 main fields within cyber security.



CLOSING CEREMONY



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الحفلة الختامية لمخيم الشبان
للامن السيبراني 2026

CYBER SECURITY YOUTH CAMP
GRADUATION CEREMONY 2026

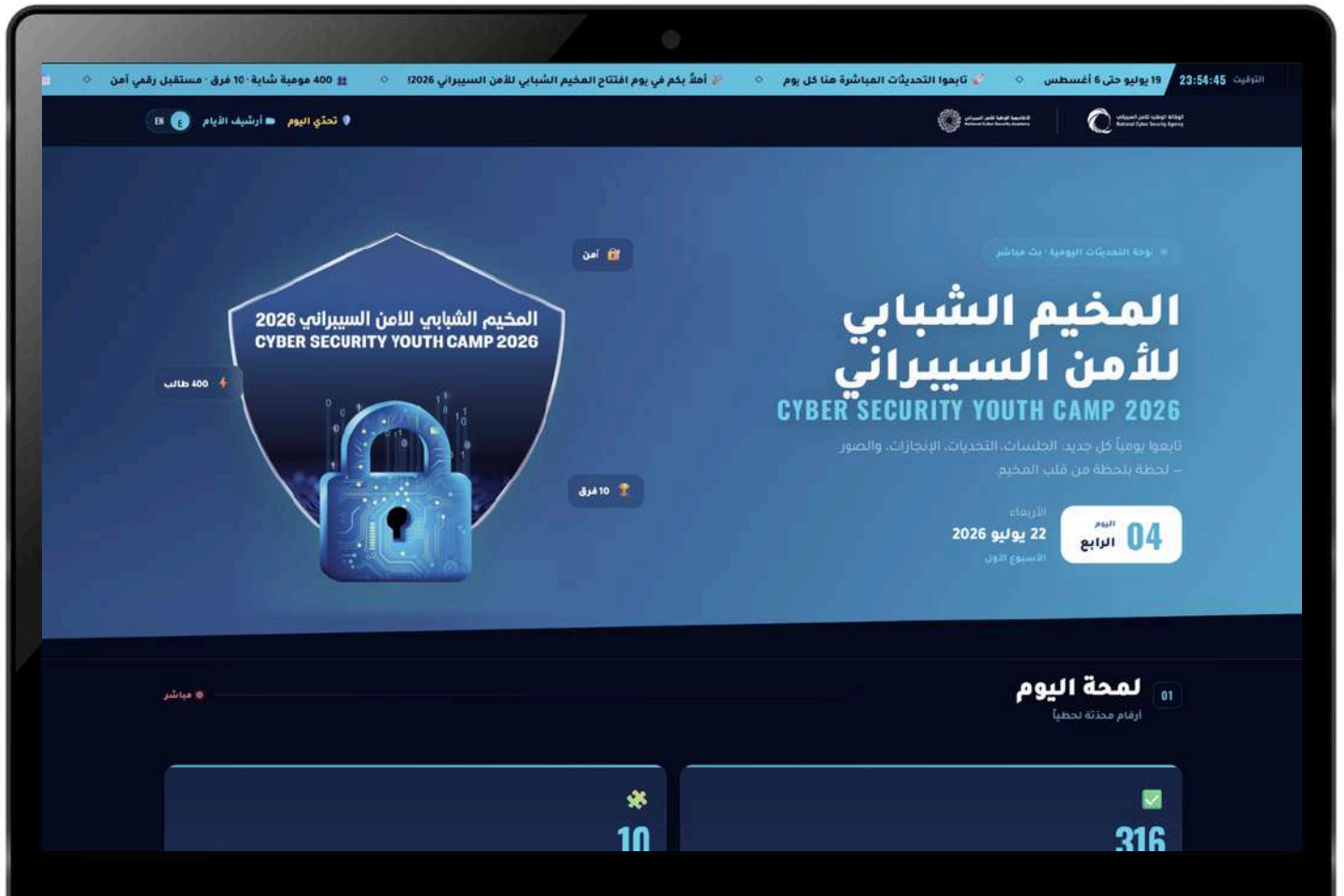


DAILY UPDATES PLATFORM

The platform was designed to be a living, interactive dashboard rather than a traditional static website, featuring:

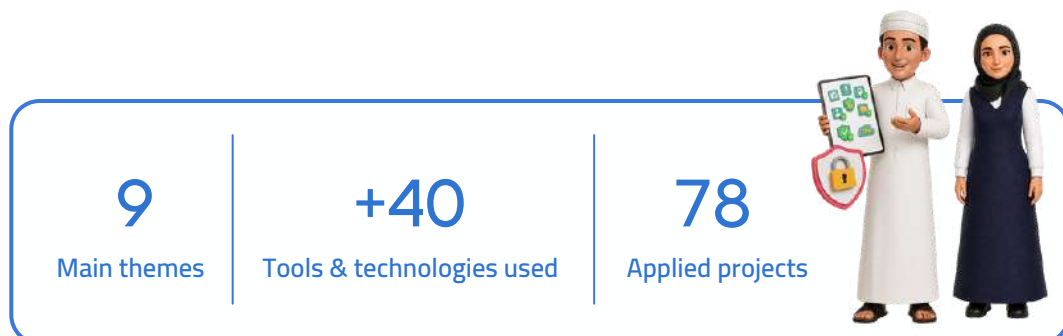
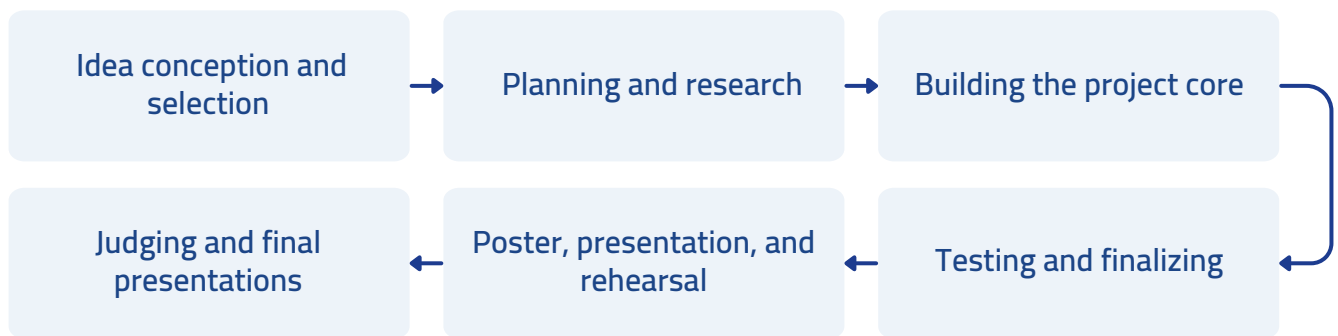
- A live schedule of training sessions for four different groups, navigable with a single click.
- Attendance and points data updating automatically from an electronic spreadsheet.
- A control panel requiring no coding, used by organizers.
- An interactive daily challenge.
- A complete archive documenting each day's activities.

This resulted in a noticeable decrease in calls from parents after the first week and helped shift their experience from anxiety to informed daily follow up through the platform.



Graduation Projects - The Project Journey

The graduation projects stage represents a pivotal phase of the camp, giving students the opportunity to apply the knowledge and skills they acquired during the training period and turn them into practical projects. This stage also helped strengthen teamwork, problem-solving, and creative thinking skills, and linked theoretical knowledge with practical application in the field of cyber security.



Key Themes Covered by the Projects

Education and interactive simulation

platforms that turn learning into a practical experience: Admins, Operation Shadow, Case Files.

Fraud and phishing detection

unified tools that scan links, messages, and fake images: CyberDeraa, Hisn platform.

Advanced defense and data protection

smart honeypots and protection of institutional data: RansomLab, QSecure, Hisn AI-Ghaz.

File and device protection

file integrity monitoring and USB media scanning: HexaGuard, FileShield, StegoVault.

LEARNING TOOLS



Platform: TryHackMe

TryHackMe is an interactive learning platform designed to enhance cyber security skills through hands-on training. The platform offers virtual labs and interactive training courses, enabling users to gain practical experience handling various cyber security scenarios.



The Handbook

A comprehensive handbook covering the entire cyber security camp content, alongside some enjoyable recreational activities. This handbook provides participants with a complete reference, allowing them to revisit the valuable information, interactive activities, and exciting challenges they experienced during the camp.

Online Training — A Reach Beyond the Hall

The in-person camp was accompanied by an open "online" training broadcast, held as two interactive sessions daily (morning and evening) covering the same camp topics. This dimension allowed those outside the limited in-person seats to follow the content and interact directly with the trainers.

11

Countries around
the world

20

Interactive sessions
(morning & evening)

1,165

Total attendance across
sessions

The online dimension added more than 1,000 new attendees to the camp's impact, from 11 countries around the world.

TRAINING CONTENT

The training content is divided into six main topics:

Fundamentals	Networks	Ethical Hacking
Web	Systems	Cyber Defense

These are covered through:



Fundamentals

Learning the basic concepts of cyber security and building a solid knowledge foundation.



Attacks

Learning how attacks and compromises occur to understand attackers' methods



Defenses

Learning how to protect against attacks and mitigate their impact



EXPERTS



As part of the camp program, interactive sessions are held where participants meet directly with a select group of cyber security experts from various sectors. These experts share their practical experience and professional insights. The sessions allow students to ask questions, seek advice, and gain valuable professional and technical knowledge, deepening their understanding of cyber security concepts and preparing them for their future paths in the field.

FIELD VISITS - OOREDOO



A field visit was organized to Ooredoo's headquarters, during which students took part in a specialized cyber security workshop. They learned about the importance of the field and its key career paths, in addition to the roles of cyber security teams within organizations, such as risk management and compliance, security engineering, and the Security Operations Center (SOC) — helping connect theoretical knowledge with real professional applications.



RECREATIONAL AND ENRICHMENT ACTIVITIES



Jewellery Making



Mirror Painting



Crime Scene Puzzle



Escape the Virus



Wireless / RC Sports



Candle-Making Workshop



Car-Building Challenge



CTF (Capture the Flag) Competition - Bank Breach - Ethical Hacking Challenge

A hands-on challenge that tests students' ethical hacking skills by solving technical challenges and exploiting vulnerabilities within realistic scenarios, enhancing their analytical, teamwork, and time-pressured decision-making skills.

Breach

A hacking group from the "dark web" managed to breach the central bank.



Recovery

Students must re-hack the bank to regain control of it.



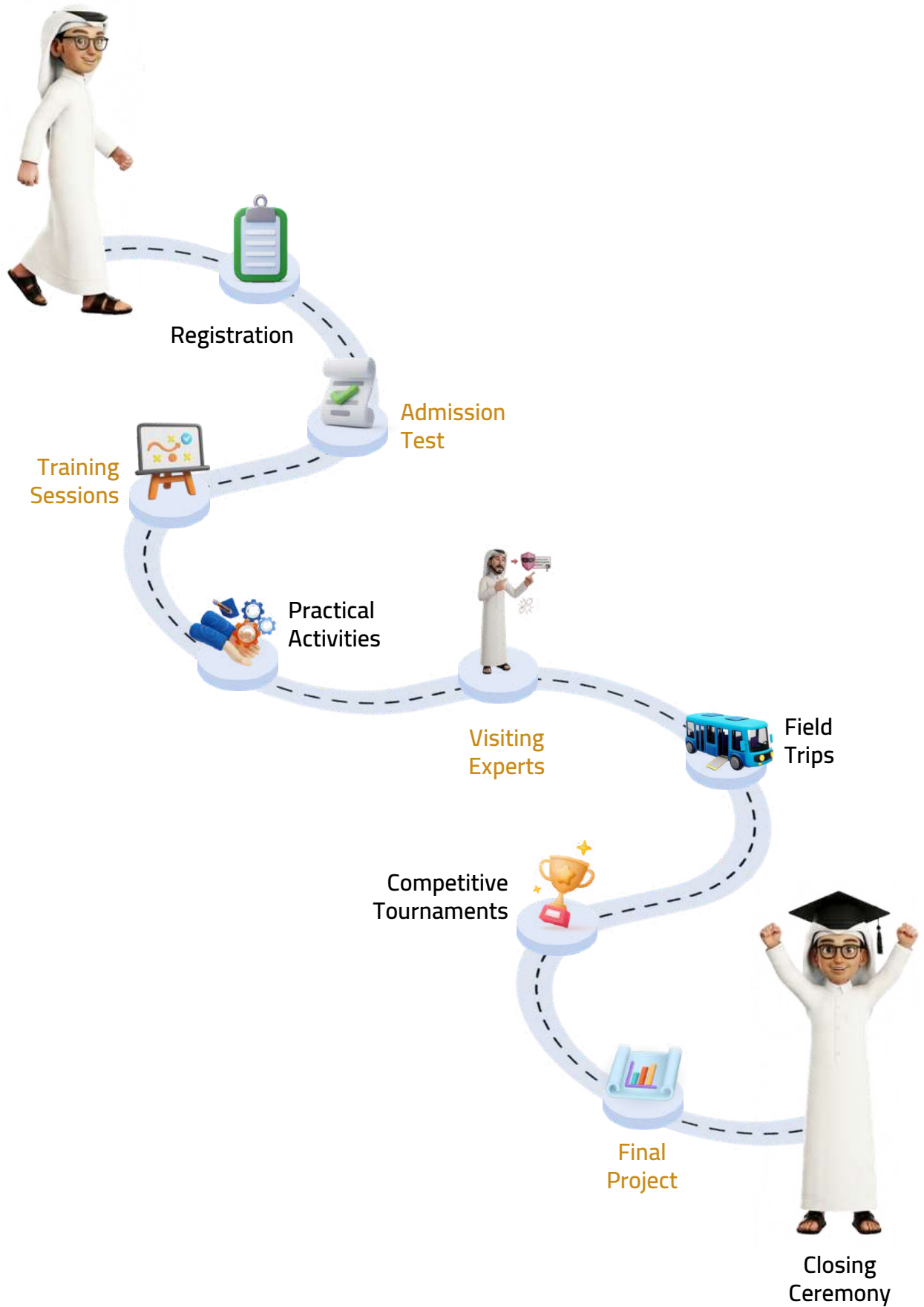
Pursuit

Students then hack the hacking group's own server to complete the mission.

Objective

To place students in a realistic scenario where they apply what they have learned in information gathering and hacking within a safe, legal framework — from reconnaissance to full control of the target — while honing team spirit and decision-making under time pressure.

STUDENT JOURNEY



PARTNERS

وزارة الرياضة والشباب
Ministry of Sports and Youth
دولة قطر • State of Qatar



وزارة التربية والتعليم والتعليم العالي
Ministry of Education and Higher Education
دولة قطر • State of Qatar



ooredoo



مدرسة قطر للعلوم والتكنولوجيا الثانوية للبنين
Qatar Science & Technology Secondary School for Boys



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency



Target Group

400

male and female students, Qatari nationals and residents, aged 13-17, from public and private schools in the State of Qatar.



Online Education

1000

Students participated online from all around the world.



Camp Timing

Three weeks

July 19th – August 6th

Girls: Sunday - Thursday, 8:00 AM – 12:30 PM

Boys: Sunday - Thursday, 1:00 PM – 5:00 PM

MISSION

To attract and embrace talented youth in cyber security, and develop their talents and skills in a way that prepares them for a promising professional future.



VISION

To attract and nurture talented youth in the field of cyber security, and develop their capabilities and skills to enable them to actively contribute to building a secure digital future.

OBJECTIVES

1

Equip students with the academic qualifications needed for admission to IT and cybersecurity colleges, and boost their job market prospects.

2

Provide an innovative training experience that blends theoretical and practical aspects using attractive interactive methods.

3

Use modern educational tools and methods based on entertainment, challenge, and innovation to enhance understanding and stimulate creativity.

4

Foster team spirit and teamwork among participants through interactive activities and competitive contests.

5

Strengthen practical and professional skills in cyber security to prepare participants to excel in their future career paths.

6

Discover young cyber security talents and guide them toward suitable career paths, contributing to the development of qualified national cadres.

INTRODUCTION

The Youth Summer Cyber Security Camp aims to prepare a promising generation equipped with the skills and knowledge needed in this vital specialty from an early age, by enabling students to explore successful career paths through integrated training programs, alongside raising awareness of the importance of cyber security and strengthening the network of relationships and communication among participants.

Lectures with Experts

Direct discussions with a select group of accredited specialists.

Practical Applications

Real hands-on training in a safe and stimulating environment.

Interactive Workshops

Practical sessions that translate concepts into direct application.

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026





الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy



CYBER SECURITY YOUTH CAMP **Executive Report**



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

CYBER SECURITY YOUTH CAMP Executive Report

