CYBER SECURITY:
COMPETITION, CERTIFICATIONS & INTERNSHIP PROGRAM

In Partnership with

FEDERAL MINISTRY OF YOUTH AND SPORTS DEVELOPMENT

HALOGEN GROUP

Proposal Date:
December 2021

EXECUTIVE SUMMARY

The initiative is a phased program across three dimensions
a. Cyber Security Competition
b. Cyber Security Certifications, and
c. Cyber Security Internship + Job Placement opportunities

Working with the Federal Ministry of Youth and Sports Development, this initiative will make concerted efforts to identify, train as well as engage youths in the field of cybersecurity and connecting the best and brightest to opportunities in the public and private sectors within and outside Nigeria.

From those that apply for this initiative, aside the prize money for the 1st, 2nd and 3rd submissions, an agreed numbers of selected youth will be offered a range of certification programs in Cyber security and also internship opportunities that may lead to permanent job placements – local and international.

Prize Awards for Competition

1st Prize
N1m

2nd Prize
N650k

3rd Prize
N350k

PHASE ONE: THE COMPETITION

The Federal Ministry of Youth and Sports Development, in partnership with Halogen Group, will be able to;

a. Identify Nigeria's next generation of cyber security professionals
b. Connect Nigeria's best and brightest to the cyber security industry
c. Create an enabling platform for skills' acquisition, youth empowerment and local contents development in the area of information and cybersecurity towards the national and economic development of Nigeria.

THE COMPETITION PROCESSES

Registration: All interested applicants are expected to register on Halogen's website. The portal will be opened for 6 weeks.

↓

All applicants will be notified via email as a confirmation of their registration.

↓

Debriefing: all applicants will receive mails before the commencement of the competition. The mail will contain:

- The scope of the topic selected.
- A template for the presentation for submission

↓

Competition Commencement

- All applicants will be given an opportunity to select a topic of their choice during the registration process.

↓

Evaluation of Submissions

- All applicants are expected to turn in their presentation/solution on or before the deadline.
- Halogen will expend 3-4 weeks to evaluate all the submissions before shortlisting the finalists for live presentation

↓

Presentation

- The list of all finalists will be published on the website.
- All the finalists will be notified via their email and all the details of the presentation will be communicated
- Each presenter has 15-30 minutes to share their solution(s).

↓

Judges

- A panel of judges with immense experience in the Cybersecurity sector will assess the solutions
- The top 3 solutions, with any others, based on the judgement of the panel of judges will be presented with the prizes and also given an opportunity to further work on their proposed solutions with Halogen's Cybersecurity Division.

Entry Criteria

- Evidence of Nigerian citizenship – NIN
- Age Range – 18 to 35 years old

COMPETITIONS

OPTION 1: Anti-Ransomeware

Ransomware is a relatively easy way for hackers to gain financial rewards, which is partly behind its rise. The accelerated digitization of many organizations, coupled with remote working, created new targets for ransomware. Thu, the volume of attacks and the size of demands increased as a result.

Extortion attacks involve criminals stealing a company's data and then encrypting it so they cannot access it. Afterward, cybercriminals blackmail the organization, threatening to release its private data unless a ransom is paid. The burden of this cyberthreat is significant given the sensitive data at stake as well as the economic impact of paying the ransom.

Ransomware attackers are becoming more sophisticated in their phishing exploits through machine learning and with more coordinated sharing on the dark web. Hackers typically demand payment in cryptocurrencies which are difficult to trace.

Task - *Build an Anti-Ransomeware that can detect, decrypt and restore.*

OPTION 2 - Multi-factor authentication (MFA)

Multi-factor authentication (MFA) is regarded as the gold standard of authentication. However, malicious actors are finding new ways to bypass it – specifically, authentication carried out via SMS or phone calls. As a result, in 2020, Microsoft advised users to stop using phone-based MFA, recommending instead using app-based authenticators and security keys.

SMS has some in-built security, but the messages sent – including for authentication purposes – are not encrypted. This means malicious actors can carry out automated man-in-the-middle attacks to obtain one-time passcodes in plain text.
This presents a vulnerability for activities such as online banking, where authentication is often done via SMS. Increasingly, we will see banks and other organizations turn towards application-based MFA.

Task – *Build an MFA Software to address this issue, with features that cater to the unreliability/vulnerabilities of applications such as Google Authenticator, Authy, e.t.c*

OPTION 3: Fraud detection

The rise of digitization, and increase in online banking, neobanks and other fintech solutions, comes the looming threat of fraud. Fraudulent activities can vary from false transactions to stolen credit cards.

One of the most common fraudulent transactions occurs when card or account information gets into the wrong hands. In principle, this sort of transactions is not all that hard to spot as they occur in locations, and volumes not readily associated with the original account owner.

Nevertheless, it can be challenging for companies with millions of transactions and/or customers to pinpoint such anomalous transactions manually or even hardcoded rules. However, this is a perfect task for a well-trained Machine Learning system (AI).

Task: *Build a fraud detection software.*

COMPETITIONS

OPTION 4 - Email Spam Detection

One of the major ways in which malware is deployed is through mails. With the rise of digitization, this threat has only proliferated. One way to combat this is through training and awareness programs. However, beyond staff awareness programs, there is a need for intelligent spam filters.

Various approaches can be taken to build a working spam filter. They all revolve around finding key words common to spam mails such as “Cash Price”, “Free Visa” and so on.

However, there is a non-exhaustive list of possible keywords, there is also the threat of wrongly classifying as spam when in fact it is legit. This is why this is a largely unsolved problem. Since rule-based solutions cannot keep up with the inventiveness of hackers, AI powered solutions are the current state of the art.

Task: Build an email spam filter.

OPTION 5 - Intrusion Detection Systems

Nowadays, it is very important to maintain a high level of security to ensure safe and trusted communication of information between various organizations. But secured data communication over the internet and any other network is always under threat of intrusions and misuses.

Therefore, Intrusion Detection Systems have become a needful component in terms of computer and network security. There are various approaches being utilized in intrusion detections, but unfortunately any of the systems so far is not completely flawless. (Hoque et al. 2012)

Task: Develop a system to spot malicious or unauthorised users on networks

PHASE TWO & THREE:

PHASE TWO: **TRAINING & CERTIFICATIONS**

Based on agreed criteria, participants from the competition will be selected to undergo training and certification programs in Cyber Security.

The Cyber Certifications are selected based on market demands and dynamics. These are internationally recognized certifications that will be deployed mainly ONLINE, thereby flexible and agile for the participants – both at basic and advanced levels. The certifications will expose and enhance skills and knowledge in cyber security and technology, whilst affording participants, additional competencies and qualifications that can position them better for employment and entrepreneurship opportunities.

	PROPOSED CYBER CERTIFICATIONS
1	Certified Secure Computer User [CSCU]
2	Certified Encryption Specialist [CES]
3	Certified Ethical Hacker [CEH]
4	Certified Penetration Tester [CPT]
5	Computer Hacking Forensic Investigator [CHFI]
6	Certified Disaster Recovery Professional [CDRP]
7	Certified Incident Handler [CIH]
8	Certified Application Security Engineer (Java and .NET) [CASE]

The above certifications are certified by our US partner – CertiProf®.

PHASE THREE: **INTERNSHIP & JOB PLACEMENTS**

The internship program will recruit a selection of the top participants during the competition and take them through a 3 months program.

Interns will work on live cases in Cyber Security and develop solutions under the guidance and tutelage of industry experts.

Intern will also attend workshops and seminars and will be further equipped with additional competencies in the following areas;

- Introduction to Enterprise Security Risk Management
- Introduction to Project Management
- Introduction to Business Development
- Entrepreneurship
- Emotional Intelligence
- Business Communication + Presentation Skills
- Work Ethics + Professional Behaviour
- Team Work
- Problem Solving Techniques

CONTACT
DAMILOLA AMODU
Program Coordinator
SST, Academy Halogen
info@academyhalogen.com