Non-Profit Partner Project

EVOLVE ACADEMY

2022

What is the non-profit partner project?

Non-profit organizations can partner with Evolve Academy to receive cybersecurity assessment work pro bono. The engagement is led by an Evolve Security cybersecurity engineer with the support of Evolve Academy students. This partnership offers cybersecurity students real work experience to supplement their training, while the non-profit receives important information to help secure their environment.

> Our assessments provide important information to help secure your environment.

Who are the students?

Evolve Academy students come from diverse professional backgrounds and are passionate about cybersecurity. Students sign NDAs and approach the cybersecurity assessment as if they were on the job, delivering the assessment and report for a paid client.

Our Graduates Work For...

What is included in the project?

Evolve Academy students will perform four assessments.

1. Internal Vulnerability Scan (IVS)
2. External Vulnerability Scan (EVS)
3. Social Engineering Campaign
4. Email Breach and Acceptable Email Use Policy Audit

Each of these assessments are built around the skills our students obtain during their studies with Evolve Academy. The engagements are vulnerability assessments, ***not full penetration tests***.

What is the difference between a vulnerability assessment and penetration test?

Evolve Academy students will assess the security posture of your organization's internal and external network infrastructure and assets, providing vulnerability analysis and remediation recommendations.

The key difference between a vulnerability assessment and a penetration test is that our students stop at the edge of your network, never gaining access to your internal resources or compromising data from privileged locations on external resources. Students will not attempt to exploit vulnerabilities, capture credentials, compromise user accounts, or otherwise perform activities that could be harmful to the organization and result in a breach of security.

What is required to be eligible for the non-profit partnership?

- An on-premises network infrastructure containing a minimum of one server and a total of 25+ workstations (laptops or desktops connected to the network).

- A public-facing website that we are allowed to scan with vulnerability analysis and information gathering tools.

- A list of 25+ employee emails you authorize us to use with the phishing campaign.

- Authorization for an Evolve Security engineer to perform a credentialed scan of your internal network using Nessus.

- The ability to meet with us on the final day of the assessment on a Thursday from 7pm - ~8pm CST for a report readout and debrief.

- The total time commitment for the partner will be a minimum of two hours and a maximum of three hours, including the report readout. The internal scan may take from several hours to multiple days, depending on the size of the network, but it does not to be actively monitored.

Assessment Descriptions

Internal Vulnerability Scan

A full time Evolve Security engineer will work with your team to run a fully credentialed scan of your internal network. This provides our students with a detailed list of your internal IT infrastructure and the associated vulnerabilities. They will use this information to deliver a report containing vulnerability remediation recommendations.

External Vulnerability Scan

Evolve Academy students will perform passive and active information gathering and vulnerability analysis on these assets. The information gained will be used to create a report detailing vulnerability analysis and remediation recommendations.

Social Engineering Campaign

Evolve Academy Students will craft several custom phishing campaigns to be sent to an approved list of employees. Our staff will work with you to define the scope of targets and approved topics for the campaign. After the completion of the campaign, the students will deliver a report containing detailed information on the success of the campaign and the campaign itself for internal training purposes.

Email Breach and Acceptable Email Use Policy Audit

Evolve Academy students will use the list of employee emails to perform a breach audit, using open-source tools to determine what users and emails are included in a data breach and the information exposed. This audit will inform your organization how well your team members are adhering to acceptable email use policies and inform future policy changes and training opportunities.

Nick Liakopulos

UCAN | CIO

> The level of professionalism and work completed by Evolve Security Academy students was outstanding. We highly recommend this partnership.

Tom Alexander

1871 | COO

> Working with Evolve was very helpful and informative. They gave us clear, concise, and current suggestions that has allowed us to improve our security operations. We look forward to continuing to work with them in the future.

Get In Touch

(312) 957-5682 ext. 3

connect@evolvesec.com

www.evolvesecurity.com