AimValley

Student Assignment

Security Tests for EDR/MDR Solution

AimValley is a world-class engineering and innovation center that designs and builds networking solutions. We are based in Hilversum, with colleagues in Canada, India and France. We started in 2003 as a spin-off from Lucent Technologies (a successor from the American company AT&T), which is why we have a strong background in telecommunication solutions and have built-up a vast expertise in real-time processor technology. Our telecom experience creates a perfect crossover to the HealthTech sector, where we are establishing our footprint, through developing innovative connectivity solutions for medical device manufacturers. Most of our design & development is done in-house.

Product development entails the preparation of requirements documents, specifications of system architecture, electronic development (board design, system certification, mechanical design), FPGA/ASIC & software development, system verification, and product/factory introduction. AimValley uses FPGAs to process high-speed transmission functions. Real-time requirements are key in our software development.

Our business is about people and our teams are dynamic, skilled and passionate about technology. Recruiting and training the right talent is an essential part of the AimValley DNA. We have over 95 employees of which 75% work as a design expert in the R&D organization. All R&D employees have a college or university-level education.

YouTube

AimValley

Student Assignment

Security Tests for EDR/MDR Solution

Project Introduction - Security Tests for EDR/MDR Solution

With over 90 employees doing complex R&D tasks in a hybrid environment of Windows clients and Linux servers a secure IT infrastructure is key. One of the major threats is a ransomware infection, which could potentially halt the R&D team for a number of days and result in data loss.
To reduce these risks AimValley is considering to move to an EDR or MDR solution for both clients and servers. To show the need for such a solution and to evaluate the EDR/MDR implementation this student assignment has been defined.

Project Description

The assignment is to first define the tests which simulate a Ransomware attack, following all the typical phases of an attack; reconnaissance, weaponization, gaining access, exploitation and exfiltration. The top 5 attacks from this moment should be selected and documented in a playbook.
Using these 5 attacks a standard configured client and server will be attacked (Red team approach) and during this process the existing monitoring tools should be used to evaluate the effectiveness of the current setup (Blue team approach).
After this an EDR solution should be enabled and configured based on the input of AimValley's IT team and a client and server with this added solution will now be attacked. Again the effectiveness of the new setup will be evaluated and compared to the earlier attach on a standard client and server.
Based on the results a recommendation should be given on further improvement or tuning of the EDR solution. Also the added value of adding the management layer to EDR should be investigated.

Keywords for this project

- > Red team attack
- > Blue team defense
- > EDR/MDR Solutions

Affinity

- > Hacking tools like Metasploit
- > Writing clear documentation

Skills

- > Windows & Linux hacking
- > Competent in English
- > Independent

Are you a student with a can-do attitude and a passion for technology?
AimValley is your company!

Why not join us today: students@aimvalley.com