8-2 Journal: Portfolio Reflection

CS-405-T5469 Secure Coding 21EW5

Michael Iyaomolere

Southern New Hampshire University

June 27, 2021

**Zero trust**

This course has been exciting and a huge blessing to me. I was able to learn about the new concept when it comes to securing applications and infrastructures. The topic I will be discussing is Zero trust. This is a strategic initiative that helps prevent successful data breaches by removing the idea of trust from an organization’s network architecture. This is simply put as “never trust, always verify.” This is done to protect the modern digital environment by utilizing network segmentation and prevention of lateral movement by providing layer seven threat and simplifying granular user-access control.

In Zero Trust, you identify a “protect surface.” The protected surface is made up of the network’s most critical and valuable data, assets, applications, and services – DAAS, for short. Protect surfaces are unique to each organization. Because it contains only what’s most critical to an organization’s operations, the protected surface is orders of magnitude smaller than the attack surface, and it is always knowable.

With your protected surface identified, you can determine how traffic moves across the organization to preserve the character. Understanding who the users are, which applications they are using, and how they are connecting is the only way to determine and enforce a policy that ensures secure access to your data. Once you understand the interdependencies between the DAAS, infrastructure, services, and users, you should put controls in place as close to the protected surface as possible, creating a microperimeteraround it. This microperimeter moves with the protect surface, wherever it goes. You can create a microperimeter by deploying a segmentation gateway, more commonly known as a next-generation firewall, to ensure only known, allowed traffic or legitimate applications have access to the protect surface.

Reference:

<https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>