Section 1: Week 1: Evaluate Cybersecurity

Nate Bachmeier

TIM-8301: Principals of Cybersecurity

April 5, 2020

North Central University

# Section I: Significant Problem

## What Problem Exists

Cybersecurity requires capabilities to defend against sophisticated attackers, which employs continuously evolving techniques that are funded by nation-states. These advanced persistent threats (APT) weaponize zero-day exploits, devise precise spear-phishing campaigns, and leverage vulnerabilities in unpatched software, among other strategies. As administrators operate within this ‘assume breach’ hostile environment, they need solutions that detect the onset of an attack and automatically augment the network topology. For example, a system might detect an unexpected yet, trusted resource is downloading sensitive information for exfiltration. That system could mitigate this scenario by identifying traffic anomalies and provisioning firewall policies to stop the attack.

## How is this problem being addressed

One realization of this vision comes from machine learning, which provides mechanisms for rule association discovery, regression, classification, and clustering. These primitives enable systems engineers to create adaptive technologies that react to implicit patterns versus explicit rules. For example, clustering algorithms can use the device’s open network ports to predict which other machines are most similar. While it might not understand that one grouping is webservers and the other malware infected zombies, the tooling enables domain experts to make informed decisions. An ensemble of algorithms could further enhance these clusters with regression analysis to detect traffic surges during off-hours and similar scenarios.

## What challenges does this create

However, it comes with a unique set of challenges where these mindless algorithms ‘do what we say, not what we mean.’ Consider how many different ways the previous same dynamic firewall example could halt production environments. False-positive scenarios could be self-inflicted, such as during the deployment of new services and features. Another outage might come from an attacker manipulating third-party traffic and triggering the quarantine remediation, resulting in a denial of service attack.

## Whom does it impact and why

# Section II: Cybersecurity Overview

1. Goal of cybersecurity
2. What challenges exist
3. Who produces these issues
4. What is the role of network security
5. What is the role of assessment
6. How do team communication and culture factor in