Dylan Coulter February 17, 2025

ID#1896062

C405

# **CS405 7-1 Journal: Consider the Motive for the Attack**

**Motive is often a mystery, but looking for motives should be a best practice. Address the following:**

**How will you apply this concept to your own practice?**

Understanding the motives behind an attack is an important part of cybersecurity. Being able to identify what may motivate an attacker can help put tactics in place to mitigate potential threats. This is a concept I intend to integrate into my own preparation by routinely analyzing and trying to identify different attack vectors and what the possible motives are. This will be a practice even if the possible motives identified seems ambiguous or obscure. We may not be able to identify every possible motive of an attacker, but doing our best to recognize what we are trying to protect and why this would be important to someone else can help us develop a more secure system.

**How would you explain this to a new developer on your team?**

When explaining this concept to a new developer it would be important to give examples as to why identifying motives are so important. I also believe there are some everyday life examples that can relate to this concept to help make the connection as to why it is important to consider when developing something. In life we always gage others motives and use this to make judgement on how to protect our interest. These connections could help a new developer make similar connection when dealing with cybersecurity. We are better of safe than sorry so the more threats and motives we can identify the better we will be at mitigating them. I would ask the new developer what, why, and how. What do we have that someone would want, why would they want it, how might they go about doing it. Identifying these things would help identify motives and threats and builds a secure robust system.

**What is one example of this concept you can use in your final reflection in Module Eight?**

One example of this concept that I can use for my final reflection in module eight could revolve around a scenario where our companies system experiences a series of arbitrary but persistent brute force login attempts. Instead of only focusing on trying to deal with the immediate threat the emphasis of the reflection would be looking further into the potential motives. The would be done be theorizing different possible motives such as credential harvesting, data theft, or even the disruption of service. With this I would investigate how gaining a better understanding of these motives could have a positive impact on out response strategies. This could be in the form of closely monitoring any suspicious login patterns and applying stronger authentication tools.