​

**Domain: Logging and Monitoring**

**Escalating Security Events**

*How do you determine if a security event or alert is important enough for escalation?*

A common question that arises when monitoring and logging traffic is, *How do you determine if a security event or alert is important enough for escalation?* To answer this question, companies need to have five foundational elements in place. First, the company’s mission and goals. This may seem basic but if a foundation is not set and a solid goal provided, security vulnerabilities and inefficiencies occur. During Project-1, our goal was to make a cloud-based network that provided tight security by allowing a limited amount of ports to be open, under the restriction of one device/IP given access. This goal guided me in laying out specific rules for inbound traffic to one device (Jump-Box VM) from one device (my personal computer). Only then, was I able to enter the network and reach the other VMs and containers. Second, a scale of prioritization. It is important for each event to be able to be categorized into a level of threat impact. If I notice traffic showing multiple attempts to enter the Jump-Box VM from a machine that is not my own would cause me to take more notice than traffic confirming that requests from my device went through properly. It is important to make for companies to be critical thinkers and honest in what will impact their service and livelihoods. When in doubt start gathering a list of scenarios and issues that have, can, and are possible to occur, then divide each item into a scale that makes sense for the company. It can be based on financial loss (i.e. Level 1: $500 or less lost to level 8: Company Goes Under). It can be based on product or service delay to customer/s (i.e. Level 1: 1 hour or less delay to Level 10: 1 month delay). Whatever scale is chosen (what is being measured, number of levels, markers to hit, etc.…), the criteria is still the same. You need to have a range that goes from minimal damage to the company to a critical damage to the company. The ranges should not be too large or small so that things are properly and efficiently handled. Third, is creating a list of vulnerabilities and prioritizing those. This list of weaknesses is an indicator of the mostly likely attacks that will occur. Once this list is developed, you can see where they fall in your scale and if the scale needs any alterations. Fourth, a policy and procedure needs to be written with technical steps in how to address and handle events that fall into each of the established categories in the scale. For example, when I see multiple denied access attempts to the network (in this case it was simulated) then I would be given checking the inbound rules I have in place in my security group, known vulnerabilities, and confirm the structure in place has not been altered and is doing its job correctly. Having resources, like Kibana, helps monitor and log traffic. It can even be set to prioritize certain items so it is easier for analysts to check actions that fall within the higher levels on the scale that was developed. Finally, the fifth element that needs to be implemented to determine if a security event is worthy of escalation is to test the scale and system that was developed. This can be done through practice sessions, but ultimately needs a full table-top exercise with little warning to the employees. The reason behind this is to see what would occur in a real-life scenario. The results from this will determine if the scale is graded appropriately and if the procedures in place are detailed enough.