Domain: Logging & Monitoring

Question 3: Escalating Security Events

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

1. The dilemma is figuring out whether or not a given security event or alert is important enough to escalate it to a higher level for further examination.

2. Provide a Concrete Example Scenario
    - We know that any sort of sudden spike in web traffic can come across as suspicious. The data from the web traffic needs to be examined to determine which type of logs are creating this spike. In the case of our project, we were able to determine the spike in traffic was a result of a Brute-Force-Attack.

      During the attack, a single source failed to login to an account more than 16,000 times within a 5 minute time span. A 401 error code is sent back each time a user fails to login, which means more than 16,000 401 error codes were generated.

      An alert should be set to notify us when a large amount of 401 error codes are sent back to a user within a small time frame. For example, an alarm was set to trip if 50 401 error codes were created within 5 minutes.

      This alarm would have been efficient enough to alert us during the attack. It is important not to set too low of a number to avoid alert fatigue, but also high enough to make sure an attack doesn't go unnoticed. The number from the example might vary depending on a company's history and current guidelines/baseline.

3. Explain the Solution Requirements
    - What kind of malicious activity does each alert suggest?

      Based on the alert, an alarm is tripped when a single user has failed to login more than 50 times within 5 minutes. The use of common knowledge

and knowing how Brute-Force-Attacks work, we can decide that this is suspicious behavior.

If I received the alert quick enough, I would find the total amount of identical logs that were created during this time and decide which action to take. If only one alert was triggered (meaning between 50-99 error codes were generated), I would escalate it to the next level, with low-normal severity. I might also check with the user (employee) if they did in fact try to login that many times. However in our case, there were more than 16,000 error codes from logs. I would immediately escalate this to the next level with HIGH severity.

How I would respond to these events might vary depending on the company's preferences and what they have seen in the past. For example, 30 failed login attempts within 5 minutes instead of 50.

4. Explain the Solution Details

   Kibana is a very useful tool in examining web traffic data, especially in large numbers. I was able to utilize Kibana's Dashboard feature which provided easy to read graphs and other vizualizations. After selecting a time frame, I was quickly able to find the massive spike in traffic from the cyber attack. With Kibana's Discovery feature I was able to get more detailed information from those logs, such as the suspiciously large amount of failed login attempts.

5. Identify Advantages and Disadvantages of the Solution

   If multiple 401 error codes were generated within a small period of time, in the best case scenario, a user forgot there password and did in fact try to login that many times and failed. In this case, If I am able to get in contact with the user (employee) fast enough and confirm with them that they did in fact fail to login multiple times, it would be safe to decide not to escalate the issue. However, that might depend on the company's baseline practices.

   If I am able to confirm that a Brute-Force-Attack occurred but was unsuccessful, I might choose to block that IP address and contact that user to reset his/her password (with 2 factor authentication, if possible), instead of escalating the issue. Again, this might depend on the company's baseline procedures.

- How would you respond if you learned that a team member "handled" an issue they should have escalated?

  If I learned that a team member "handled" an issue they should have escalated, I would immediately escalate it if it hasn’t already. Out of respect to the team member, I might have them send the escalation themself. I would try to explain to them why the event needed escalation while providing an example of a worse case scenario result. All while keeping a positive vibe in our work environment.