Alexei Hooks

IST 456

Professor McIntier

February 12, 2022

Exercise 1

As asked of me, I have researched and added insight into issues within the modern information security business landscape. New threats and vulnerabilities are always being found or created, and it is an information security expert's job to assess and adapt to them. When starting my research, I was directed to "databreachtoday.com" to start my search through different threats and vulnerabilities. This search provided me to a video discussion led by Tom Field entitled, "Modern Threat Detection and Response: The Challenge." In the video, Mr. Field interviews and talks to Partha Panda, CEO and Co-Founder of CySiv, a 24/7 Threat Detection and Response company based in Texas. A point that was brought up as a threat was the case of false positives in the field of data security.

Security teams of today are overwhelmed with data from many different places. With this comes a heightened risk of missing a key piece of data that could lead to shutting out an attack. False positives add to the workload of these analysts and could potentially pave the way for an attack to occur. These events are defined by NIST as "An alert that incorrectly indicates that a vulnerability is present" (nist.gov). Partha Panda said that the issue with false positives is the "volume of data. As it will only get worse every day, we have more device connections added to a network" (databreachtoday.com). He went on to explain that the true need is efficiency, as professionals need to know what is really important, and what is a waste of time. He calls false positive "noise" as it only adds chaos to an already hectic task. Panda explained that the real, "actionable," threats are those that need to be taken care of immediately or adverse events would occur. By stepping in the way of these events from happening, the system can avoid unwanted issues or attacks. That is why the problem of false positives in a security system are important to take care of.

In the article, "Cybersecurity 101: What You Need To Know About False Positives and False Negatives," from Infocyte.com, an overview of false positives, and an analysis of how to properly mitigate the threat was offered. The overview of false positives was close to Panda's explanation but added the statistic, "false alarms (positives) account for roughly 40% of the alerts cybersecurity teams receive on a daily basis" (infocyte.com). This stat was revealing to how widespread false positives are, and how mitigating the threat of them can save a business' time and resources. Infocyte.com also released information curated to help strengthen a company's vulnerabilities and mitigate the risk that comes with false positives. Skills that were mentioned to strengthen were items such as proactively searching for breaches within your system, educating your employees on the best practices on how to avoid spending time on false positives, and increasing your devices to speed your detection time. Each of these practices could be used in a way to more efficiently discover and locate real threats, and push the false positives away in a quicker fashion.

By increasing your company's speed and security, you set yourself to be in a good position against threats. This allows you to have more freedom and move to be proactive in finding possible risks, and patching them to full secure the organization.

References

Cybersecurity 101: What you need to know about false positives and false negatives. Infocyte. (2021, August 10). Retrieved February 13, 2022, from https://www.infocyte.com/blog/2019/02/16/cybersecurity-101-what-you-need-to-know-about-false-positives-and-false-negatives/

Editor, C. S. R. C. C. (n.d.). False positive - glossary. CSRC. Retrieved February 13, 2022, from https://csrc.nist.gov/glossary/term/false_positive

Field, T., &amp; Ross, R. (n.d.). Modern threat detection and response: The Challenge. Data Breach Today. Retrieved February 13, 2022, from https://www.databreachtoday.com/modern-threat-detection-response-challenge-a-17915?highlight=true#dynamic-popup