Adam Donner

Web 430

Assignment 8.3

October 30, 2019

Telemetry is an automated communications process by which measurements and other data is collected and transmitted for monitoring of a system (Sumo Logic, 2019) Telemetry plays a significant role in security. Every day there is an alarming number of active cybersecurity threats. No matter how good an organization's cybersecurity team is, they could never be able to manually detected the number of threats that they get on a daily basis. Automation is essential in identifying attacks from threats and discovering anomalies for more in-depth analyst review (Shames, 2018).

Security telemetry that has been created in an application can detect problematic user behavior that could lead to fraud or unauthorized access. Examples of these areas include user passwords, user email address resets, user credit card charges, or successful and unsuccessful user login attempts. In addition to the security telemetry, there needs to be alerts created around essential events to ensure that issues can be detected and corrected quickly. Along with the application, it is also important to create telemetry in the environment to help detect unauthorized access early on. This is especially true for the components that are running the infrastructure (Kim, Debois, Willis, Humble, & Allspaw, 2017)

Logs and security go together; all compliance frameworks require them to some degree. Security is using the logs for forensics as well as to determine what actually went wrong. This can be done after a breach has occurred and for trying to figure out how access was gained in the first place. There are some challenges when using logs for application security. Some of these challenges include delayed response means delayed decision, limited data, and limited context. Being out of band of the application means that any application security issues and the necessary response will inherently have a delay. When the data is limited, it means that there is a limited amount of insight that will be available. A limited amount of context means that there is a limited amount of understanding to determine if the breach was a casual internet-wide bot or a persistent attacker trying to get access to the database (Wickett, 2017).

There are many benefits to creating security telemetry in applications. DevOps team can benefit from telemetry by seeing the feedback from updates or changes in the applications. The security teams can use telemetry to establish a report-based dashboard that can monitor any threats to the application. The hosting teams can benefit from the real-time alerts and notifications that come from possible advanced threats. The uses of the application also benefit from security telemetry in the application. The users benefit from the confidence that the application is being continually monitored and has integrity. Cloud-based application benefit mainly from this (Amoroso, 2017)

Creating and establishing security telemetry in applications should be considered a best practice or any DevOps team. Security telemetry will look for suspicious user activity, any out-of-band network access, or unusual database activity to detect hacking incidents before they become security breaches.

References

Amoroso, E. (2017, February 10). Using Telemetry to Secure Applications. Retrieved October 29, 2019, from <https://www.tag-cyber.com/analysis/articles/using-telemetry-to-secure-applications>.

Kim, G., Debois, P., Willis, J., Humble, J., & Allspaw, J. (2017). The DevOps handbook: how to create world-class agility, reliability, and security in technology organizations. Portland, OR: IT Revolution Press, LLC.

Shames, A. (2018, October 10). Threat Intelligence, Security Telemetry for Targeted Attacks. Retrieved October 29, 2019, from <https://www.lookingglasscyber.com/blog/tech-corner/cto-series-assessing-targeted-attacks-using-network-activity-part-1/>.

Sumo Logic. (2019, May 21). What is Telemetry? The Guide to Application Monitoring. Retrieved October 29, 2019, from <https://www.sumologic.com/insight/what-is-telemetry/>.

Wickett, J. (2017, February 9). Why Logs aren't Enough for Security. Retrieved October 29, 2019, from https://www.signalsciences.com/blog/why-logs-arent-enough-for-security/.