**Faye Van Roekel**

**February 20, 2020**

**Web-430**

**Creating Security Telemetry in an Application**

It has become common in our everyday lives to have cybersecurity threats. There are so many threats that it would be nearly impossible for humans to be able to detect all of the threats that are present. Security telemetry in an application is a communication process that is automated. Within this process there are measurements and other data which is collected. The data is then transmitted for monitoring the system or application.

Problematic user behavior can lead to fraud or unauthorized access to applications. This unauthorized access can be obtained through user passwords or email address resets, credit card changes, and sometimes through unsuccessful user login attempts. Security telemetry can be created within the application so it can find problematic user behavior and alert or transmit the information. Alerts are created around essential events within the system. This ensures that the issues are 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, Humbe, & Allspaw, 2017).

Many compliance frameworks require logs. Logs and security go hand in hand. The logs can be used to determine when and how the problem occurred. After a breach happens, logs are reviewed to figure out how unauthorized access was gained. When logs are not kept up or reviewed regularly it can delay decisions or give a picture with limited data or context. Server logs are an important source of data that can be regularly analyzed to help prevent security breaches.

Two-factor authentication is something that is becoming more common as a telemetry use. This is something that the agency I work for uses. When we log into our computers, we have an authentication message sent to our cell phones that we need to select and say it is us entering the account. The two-factor authentication is an extra layer of security. After the user logs in with their password, they might have a second factor that they would have to prove that they are the correct person to access the account.

DevOps teams benefit from telemetry by seeing the feedback from updates or changes within applications. There are many benefits when there is security telemetry present in applications. Telemetry is used with security teams to establish report-based dashboards that monitor threats to applications. Teams benefit from real-time alerts and notifications that sometimes come from possible advanced threats. There is confidence with users when they know the application is being continually monitored. Telemetry should be a something all DevOps teams utilize.

**References:**

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.

Amoroso, E., (2017, February 10). Using Telemetry to Secure Application. Retrieved February 20, 2020, from <https://www.tag-cyber.com/analysis/articles/using-telemetry-to-secure-applications>

Sumo Logic. (2019, May 21). What is Telemetry? The Guide to Application Monitoring. Retrieved February 20, 2020, from <https://www.sumologic.com/insight/what-is-telemetry/>