|  |  |
| --- | --- |
| Poster 0000 (Do NOT edit this line) |  |
| LCARS: Lightweight Cloud Application for Realtime Security | |
| Authors: | Advisor: |
| **Mariah Molenaer, Graham Burek** (Mariah.Molenaer1@Marist.edu,  Graham.Burek1@Marist.edu)  School of Computer Science  and Mathematics  Marist College  Poughkeepsie, New York | **Alan G. Labouseur**  (Alan.Labouseur@Marist.edu)  School of Computer Science  and Mathematics  Marist College  Poughkeepsie, New York |
|  | |
| We present LCARS: the Lightweight Cloud Application for Realtime Security. LCARS is a web based security application designed to identify, analyze, respond to, and help prevent realtime attacks and threats targeting our network infrastructure. In recent years, network-based cybersecurity attacks have increased in both frequency and severity, far outstripping traditional defense methods. LCARS addresses this problem. We collect attack data from LongTail [1] honeypots and other network monitoring devices and logs, which we parse into JavaScript Object Notation (JSON) for analysis by our analytical tools. One such tool is BiG\* Data Studio [2], which allows us to visualize attack logs as force-directed graphs and execute graph queries for easy identification of top influencers. Other tools include hive plot visualization and translation to relational data. In order to respond to these attacks, we have implemented a threat intelligence database comprised of attack profiles, response recipes, and orchestrated responses. A response recipe consists of a collection of firewall rules, while an orchestrated response maps an attack profile to one or more response recipes. LCARS enables us to easily deploy orchestrated responses through utilization of RFW (Remote Firewall) [3], an open-source REST API for iptables. LCARS is primarily written in JavaScript, but also employs our own REST API written in Java, which enables communication with our relational database and other server-side processes. Our poster will detail these and other architectural decisions we made in developing this system as well as our software development efforts relating to collecting log data, parsing it into JSON, producing hive plot visualizations, generating graph and relational representations of our data, and building the threat intelligence database and it’s associated API. This work is sponsored by NSF Grant Award number 1541384 CC\*DNI Integration: Application Aware Software-Defined Networks for Secure Cloud Services (SecureCloud) [4].  References:  [1] LongTail. http://longtail.it.marist.edu/honey/. Accessed January 29, 2017.  [2] Alan Labouseur, Shane Crumlish, Cassandra Graves, Melissa J. Iori, Gregory Miller, and Thomas J. Wojnar. 2016. G\* studio: an adventure in graph databases, distributed systems, and software development. ACM Inroads 7, 2 (May 2016), 58-66.  [3] RFW. https://github.com/securitykiss-com/rfw. Accessed January 29, 2017.  [4] NSF CC\*DNI Grant. https://www.nsf.gov/awardsearch/showAward?AWD\_ID=1541384. Accessed January 29, 2017. | |