Using OpenSearch to Achieve M-21-31

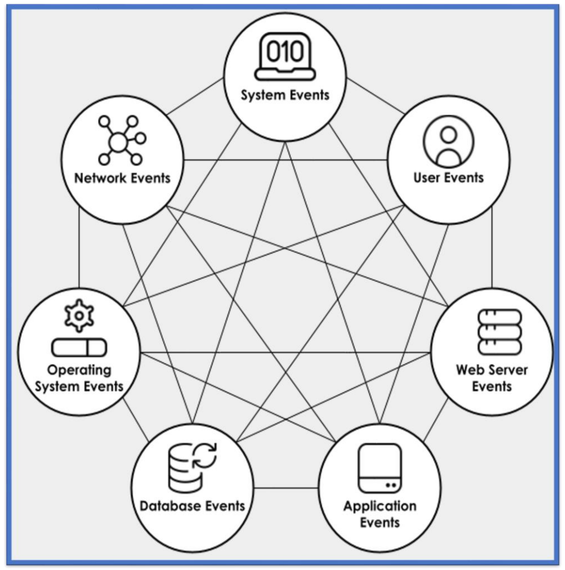
FERMILAB-POSTER-24-0154-STUDENT

Isaac R. Birgen, *Lewis University*, Under the Mentorship of Kevin Hill and Jeny Teheran

Security and Emergency Management Division, Cybersecurity Team, Fermi National Accelerator Laboratory, Batavia, Illinois 60510

M-21-31

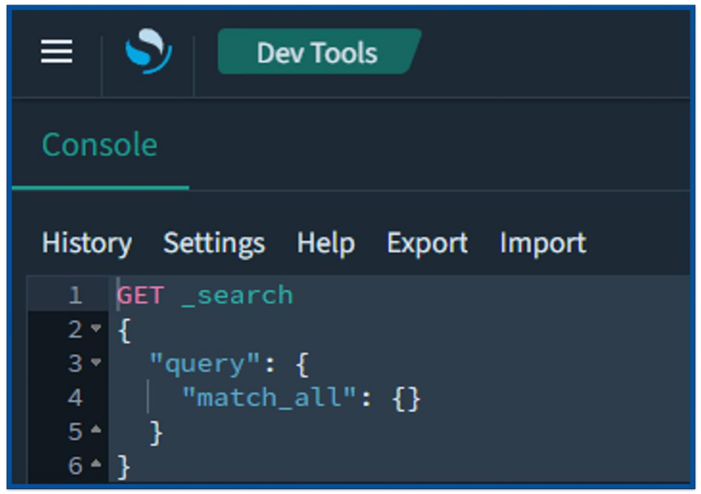
Across its three maturity levels, M-21-31 requires many different event types to be logged. Following CISA's guidance for implementing M-21-31, Fermilab is prioritizing collection and storage of logs from high-value assets along with internet-facing systems. Fermilab operates a Central Logging Facility to enable auditing, correlation, retrieval, storage, and automated alerting.



A chart showing the different places Event Logs can come from

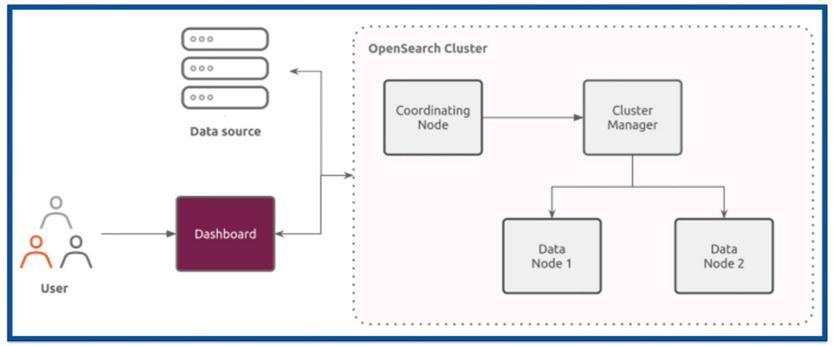
OpenSearch is an **open-source logging tool**, used by Fermilab's foreign partner CERN, that provides **free logging features** similar to that of Elasticsearch. I researched this new technology and implemented a test environment to show off the functionality of OpenSearch and how OpenSearch could be used to achieve M-21-31 compliance.

Structure of OpenSearch



The Dev Console on OpenSearch Dashboards. The Console can be used to send a single command to every node on the network

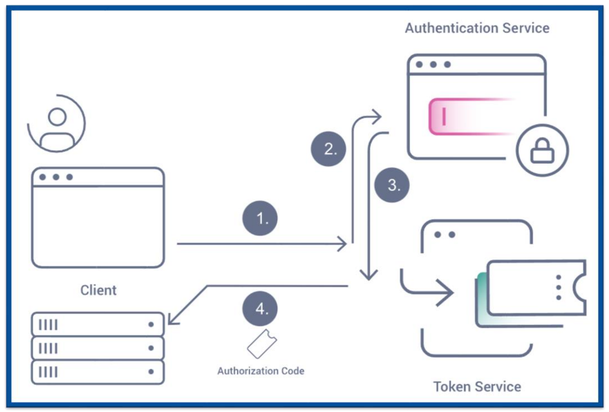
OpenSearch contains three separate technologies: OpenSearch, OpenSearch Dashboards, and Logstash. **Logstash** handles **ingestion**, **OpenSearch** is the **SIEM** for the stack, and **OpenSearch Dashboards** provides **monitoring** and data **visualization**. In addition to the stack, OpenSearch employs **clusters** to allow **companies of all sizes** to use it. This is also good for the **scalability** of OpenSearch as to increase the load it can handle one must simply add more machines to the cluster.



A simple diagram showing how OpenSearch works at a high level.

Authentication and Encryption

In addition to structure, I also investigated **authentication** for OpenSearch. I saw that it has many choices for authentication such as OpenID Connect, SAML, LDAP, JSON Web Tokens, Proxy-based authentication, and basic HTTP authentication. OpenSearch also provides **encryption** for data in transit using the TLS protocol, covering both client-to-node and node-to-node encryption.



A diagram showing the method OpenID Connect uses with OpenSearch to authenticate users

Future With OpenSearch

Beyond these basic features, more OpenSearch tools help with achieving **M-21-31 compliance**. For instance, I look forward to implementing **Cross-cluster search** which is a way for companies to **securely share data** to allow faster detection time in **incident response**. I also wish to explore OpenSearch's **machine-learning** options to permit the detection of trends that workers may miss.

This project has given me insight into the way security teams look at new tools and verify that said tools fit in with the rest of their infrastructure. I've also learned about M-21-31 and the importance of keeping and checking logs.

This research was supported in part by the U.S. Department of Energy Omni Technology Alliance Program, administered by the Oak Ridge Institute for Science and Education.

This work was produced by Fermi Research Alliance, LLC under Contract No. DE-AC02-07CH11359 with the U.S. Department of Energy. Publisher acknowledges the U.S. Government license to provide public access under the DOE Public Access Plan DOE Public Access Plan