FERMILAB-POSTER-24-0155-V

A General Framework for Modernizing Logging and Monitoring

Fatima Sanih, *The City College of New York*, Under the Mentorship of Kevin Hill and Jeny Teheran

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

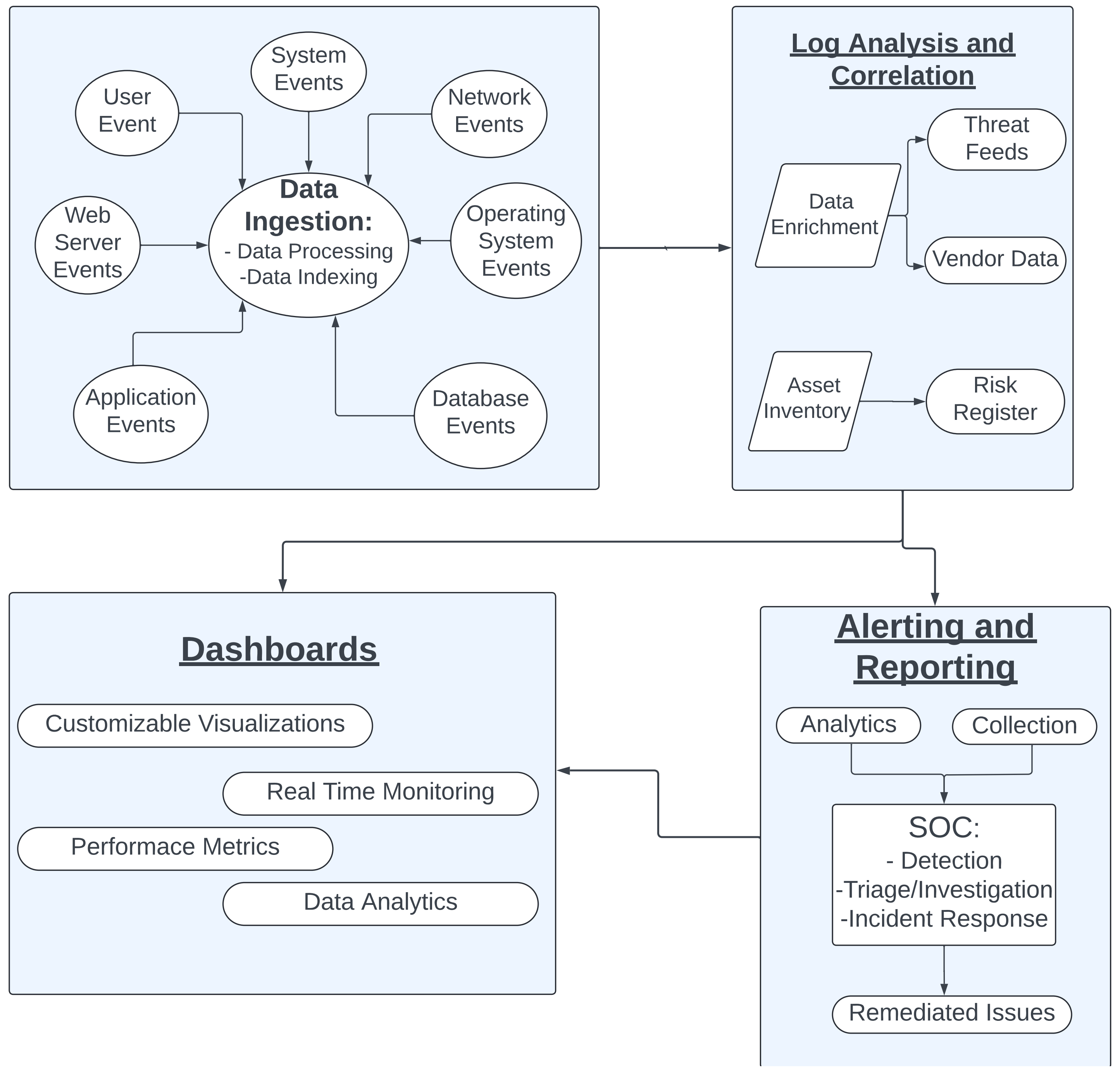
Introduction

Logging and monitoring involve the collection, storage, and analysis of data across different systems. These processes enable organizations to detect, investigate, and remediate issues, ensuring system performance, security, and operational efficiency.

Modernizing these practices not only enhances efficiency through streamlined log management but also improves security with advanced techniques that bolster an organization's incident response capabilities and future-proofs infrastructure for technological advancements, ensuring long-term resilience and scalability. Overall, it makes it easier for organizations to share information about security incidents, collaborate with partners, and respond to threats.

Key Component of Modern Logging and Monitoring

In modern logging and monitoring infrastructures, multiple components work together to ensure efficient data handling and analysis. Key components are shown below to illustrate how data flows from ingestion to processing, storage, and visualizations.



User Event

System Events

Network Events

Web Server Events

Data Ingestion:
- Data Processing
-Data Indexing

Operating System Events

Application Events

Database Events

Log Analysis and Correlation

Data Enrichment

Threat Feeds

Vendor Data

Asset Inventory

Risk Register

Dashboards

Customizable Visualizations

Real Time Monitoring

Performace Metrics

Data Analytics

Alerting and Reporting

Analytics

Collection

SOC:
- Detection
-Triage/Investigation
-Incident Response

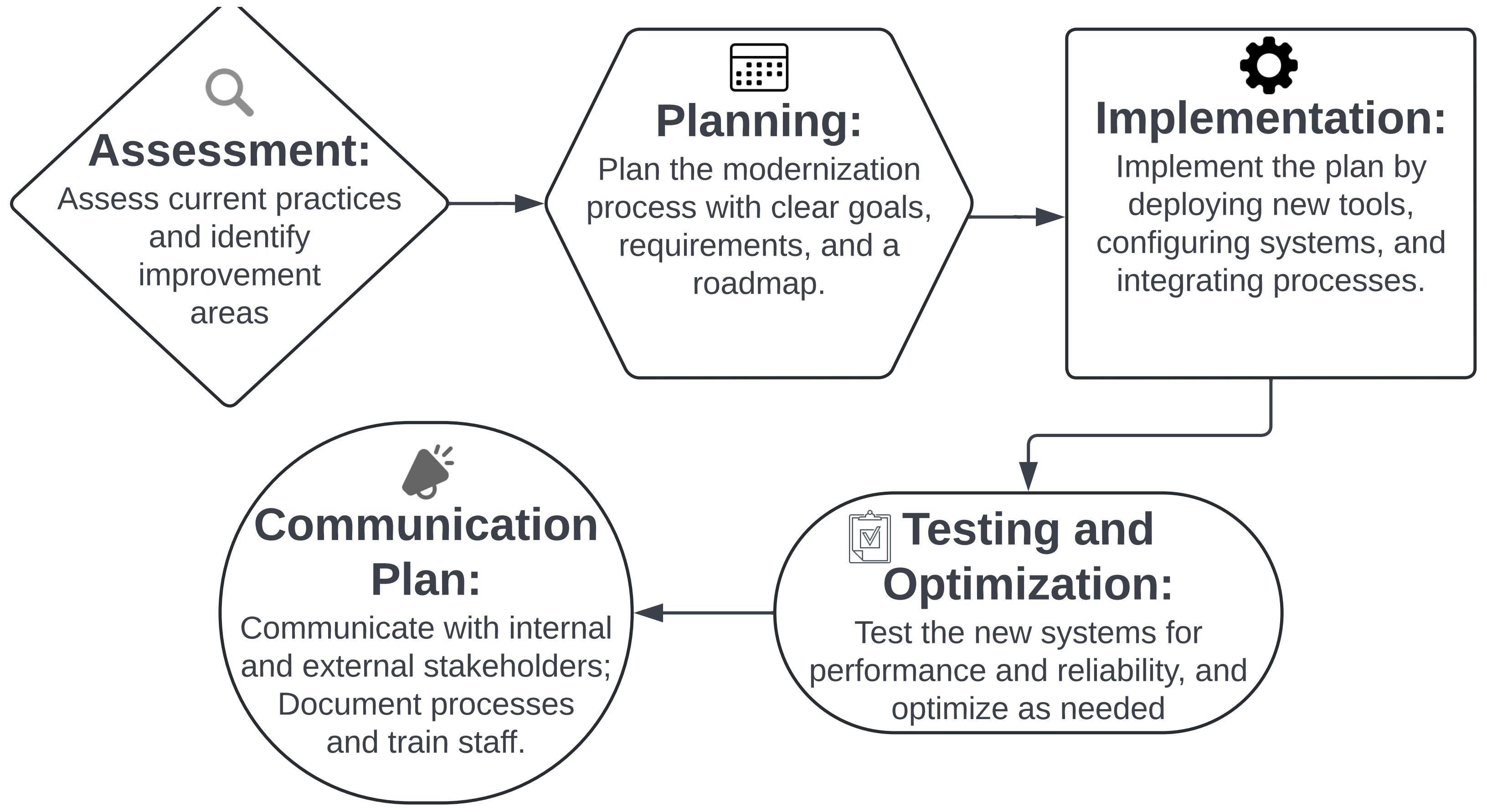
Remediated Issues

Overview of Modernizing Logging and Monitoring Workflow

1. **Storage and indexing:**
   It is the method used for storing and organizing log data for easy access and retrieval to allow organizations to manage large volumes of data efficiently and quickly locate important information.
2. **Log analysis and correlation**
   This involves examining log data to detect trends, identify anomalies, and correlate events to help organizations uncover issues and potential security threats by highlighting system performance and event patterns.
3. **Alerting and reporting**
   Focuses on generating alerts and creating reports based on log data to supports timely incident responses for effective decision-making.
4. **Dashboard design**
   It involves creating visual interfaces for displaying log data and system metrics to help stakeholders quickly understand system health and performance through clear visualizations.

Steps for Modernizing Logging and Monitoring

1. **Assessment:**
   The first step in modernizing your logging and monitoring infrastructure is to assess your current practices and identify areas for improvement. This involves evaluating existing systems, processes, and tools to understand their effectiveness and limitations.
2. **Planning:**
   Once you've assessed your current setup, the next step is to develop a strategic plan for modernization. You set clear goals, define requirements, and create a roadmap for implementing new solutions and technologies.
3. **Implementation:**
   With a plan in place, you execute the strategies and solutions defined in your plan. This step involves deploying new tools, configuring systems, and integrating new processes.
4. **Testing and Optimization:**
   After implementation, the next step is to test the new systems and optimize them for performance and reliability. This involves evaluating the effectiveness of the new solutions, identifying any issues, and making necessary adjustments.
5. **Communication Plan:**
   Finally, you develop a comprehensive internal and external communication plan that includes documentation and training. This plan involves creating detailed documentation for new systems and processes, training staff to use the new tools and follow updated procedures, and establishing channels for communication.



Assessment:
Assess current practices and identify improvement areas

Planning:
Plan the modernization process with clear goals, requirements, and a roadmap.

Implementation:
Implement the plan by deploying new tools, configuring systems, and integrating processes.

Testing and Optimization:
Test the new systems for performance and reliability, and optimize as needed

Communication Plan:
Communicate with internal and external stakeholders; Document processes and train staff.

Flowchart of the Steps for Modernizing Logging and Monitoring

From Theory To Practice

This summer, I applied modern logging and monitoring principles to assess and enhance Fermilab's existing infrastructure. The process began with an evaluation of their current system to identify strengths, weaknesses in their logging and alerting capabilities. This assessment included documenting existing dashboards, alerts, and saved searches, and analyzing the effectiveness of their log collection and management practices. Based on this review, I developed a strategic plan to transition from their existing systems to a more advanced solution, focusing on maintaining critical features such as alerts and log analysis.

These principles not only guided my approach but also ensured that the modernization process was both strategic and effective, addressing Fermilab's needs and preparing them for future challenges.

Conclusion

In conclusion, modernizing logging and monitoring infrastructure is a vital endeavor for any organization looking to enhance its security and efficiency. This project showcased how foundational principles of modern logging and monitoring can be effectively applied to real-world scenarios. Through assessment, strategic planning, and meticulous implementation, I was able to guide Fermilab through a successful modernization process.

Given more time, I would further refine the monitoring processes by integrating machine learning algorithms to predict potential security threats. Additionally, I would expand the scope of the project to include an analysis of user behavior patterns, enhancing our ability to detect activities in real-time. With the knowledge I have gained, I am now equipped to lead similar modernization efforts in other organizations, ensuring they achieve a robust logging and monitoring infrastructure.

NYU

Oak Ridge Institute
for Science and Education

DOE Omni Technology Alliance
INTERNSHIP PROGRAM
de omnibus dubitandum
Be suspicious of everything

This research was supported in part by the U.S. Department of Energy (DOE), Omni Technology Alliance Internship Program. The program is championed by the DOE's Office of Chief Information Officer (OCIO) and represents a partnership with the leadership of the Office of Economic Impact and Diversity, the Office of Science, the Office of Nuclear Energy, and the National Nuclear Security Agency. The program is 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