FERMILAB-POSTER-23-235-V

Improving Knowledge Base With Network Architecture Diagrams

Ethan Blum, University of South Alabama, Under the Mentorship Angela Correa and Jeny Teheran
Security and Emergency Management Division, Cybersecurity Team, Fermi National Accelerator Laboratory, Batavia, Illinois 60510

Knowledge Base

In order to ensure Cyber Security Team (CST) has access to updated and in-depth information regarding Fermilab systems, capabilities, procedures, tools, and training, the CST created the Knowledge Base. This consists of a wealth of information for current and future CST employees to improve knowledge retention and transfer. The Knowledge Base, however, uses outdated network diagrams that lack many of the previous and upcoming changes to the architecture. For this reason, updated diagrams have been created to reflect the current position of the CST capabilities. By employing the knowledge learned at Fermi National Accelerator Laboratory, three diagrams have been created to highlight the current state of the CST's operations and capabilities.

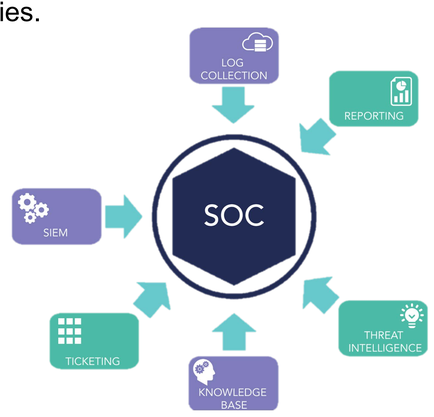


Figure 1 – Outlook of the current CST Knowledge Base information gathering. [1]

Network Diagram Process

To create a current network diagram, previous network diagrams will be analyzed and discussed with current members of the CST to figure out any changes or updates that have taken place since the outdated diagrams were created. A list of changes is compiled and reviewed by management.

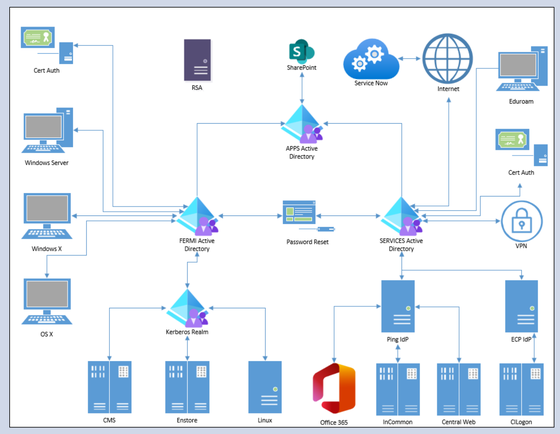
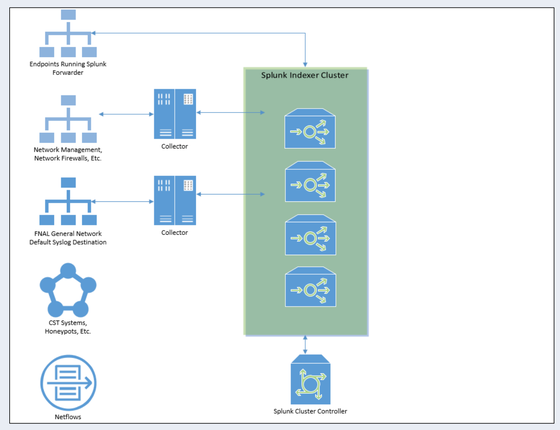
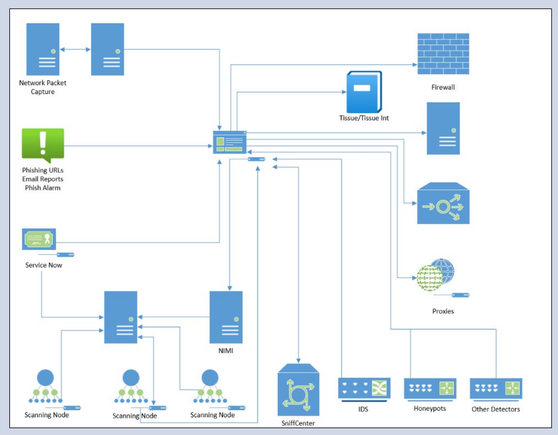
To create the diagram, Microsoft Visio is used. By using Microsoft Visio, the workflow of creating and tweaking diagrams is streamlined.

Once a platform is chosen to create the diagrams, the list of changes to previous diagrams is implemented. The diagrams include the names of devices along with the services running on the device. The diagram is then checked by management and ranking members of CST.

Incoming Technologies

These figures will allow us to easily update the diagrams as the technology is implemented. New government mandates require Fermilab to impose stricter requirements for logging. Technology such as a Security information and event management (SIEM) is under procurement and implementation. Another technology under implementation is the Security Orchestration, Automation, and Response (SOAR) system along with other logging improvements.

Created Diagrams

Created Diagrams	Highlights	Design
Authentication Diagram	• Updated Authentication Diagram • Partnered with the Authentication Team • Learned about Kerberized Secure Shell (SSH) • Figured out how certificates flow through the network	
Logging Diagram	• Updated logging infrastructure • Gained access to Splunk training • Learned about Honeypots, Blackhole routers, etc. • Learned how to analyze logs coming from network traffic.	
Scanner Farm Diagram	• Learned how scans are processed • Discovered the methods Cyber Security Team (CST) uses to scan the network • Learned about Networking Information and Monitoring Infrastructure (NIMI)	

Conclusion

The Knowledge Base ensures that the CST will have information for future training sessions. This project displayed the innerworkings of the CST and the greater Fermi National Accelerator Laboratory. It fostered a deeper understanding of the creation and upkeep of network diagrams. Future developments are needed to ensure that the diagrams are kept up-to-date as new technology is put into use.

Acknowledgements

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

[1] "security-operations-center," Next Security Solutions, Apr. 22, 2018. https://nextsecurity.co/security-operations-center/ (accessed Jul. 26, 2023).