H4DIPLOMACY

Data Architecture for Cybersecurity

SPONSORING ORGANIZATION

Bureau of Diplomatic Security (DS), Cyber and Technology Security (CTS) Directorate, Office of Cyber Monitoring and Operations

CHALLENGE

Network defenders in the Office of Cyber Monitoring and Operations need a better way to query and correlate data in a hybrid and multi-cloud data ecosystem in order to develop analytics capability at the network defender level and inform insight-driven decisions on cybersecurity incident response at the senior leadership level.

TEAM RECOMMENDED SKILLSETS

Data science, data analytics, data architecture, IT operations/infrastructure, cloud, algorithms, software engineering, database administration

RELEVANT CONTEXT

- The Department of State (DoS) relies on secure and reliable information systems and data to spread democracy, promote diplomacy, and effectively represent the people of the United States throughout the world.
- Network defenders are individuals in the Office of Cyber Monitoring and Operations who work to prevent and respond to threats to the Department's computer networks.
- Historically, the security team at CTS has deployed Security Information and Event Management (SIEM) tools that connected to DoS systems to capture all necessary data and correlate data from separate locations.
- In recent years, teams across DOS have started to establish their own cloud and disparate networks that house key data necessary for security monitoring.
- There is a lack of data uniformity and retention across different data repositories, which impedes CTS's ability to correlate data. Network defenders who query data for incident response must spend more time querying data and still risk missing key insights.
- Memorandum 21-31 established baseline log category collection and retention requirements for security event logs, further increasing the overall operating cost to conduct incident response using SIEM tools.

IMPACT

The ability of network defenders in CTS to effectively respond to cybersecurity incidents has far-reaching geopolitical consequences, and being able to make the best possible decisions in the interest of the US and foreign partners can save lives, protect information, and prevent future conflict.

POTENTIAL BENEFICIARIES

Network defenders, including threat hunters, incident responders, and incident handlers; owners of data repositories and data lakes; Senior Federal leadership and decision makers.

RESOURCES

Security Information and Event Management
Memorandum 21-31