FDA Enhances Cybersecurity to Safeguard Health Data and Systems

Introduction

The U.S. Food and Drug Administration (FDA) is ramping up its cybersecurity efforts to protect its network and systems from escalating threats.

With a central role played by the Continuous Diagnostics and Mitigation (CDM) Senior position, the FDA is adopting advanced tools like Splunk, Nessus Tenable, and CrowdStrike. This initiative aims to enhance visibility across government networks, the Splunk dashboard and aligning with government mandates for continuous monitoring, the FDA is strengthening its cyber defenses to safeguard critical health information and systems.

Our Impact

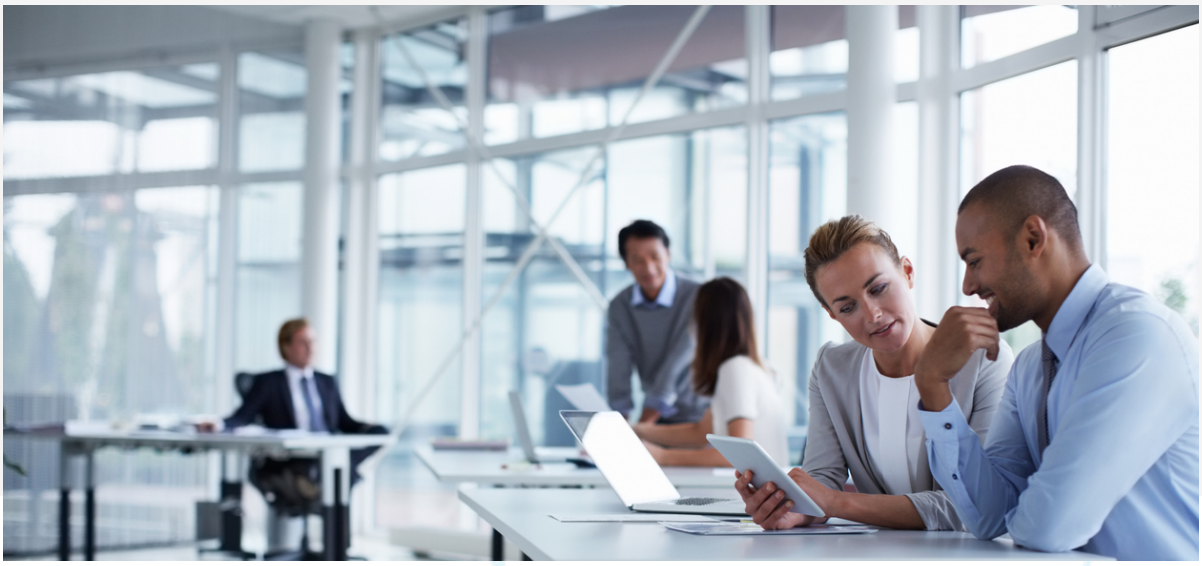
MDC Global Solutions is providing CDM and Ongoing Authorizations (OA) support services at the FDA. For the Office of Information Security (OIS), we are expanding the OA program via automation by performing tool configuration and tuning to integrate and ingest cyber data into platforms to be accessed by the various cybersecurity functional teams.

Activities performed include:

- Tool configuration and development support
- Requirements analysis
- SIEM data analysis
- Data visualization
- Data Ingestion
- Workflow development
- Database Management and support
- Security Control Testing
- Cyber Risk Management
- Executive Reporting

Conclusion

The FDA's CDM initiatives have significantly enhanced its cybersecurity posture, employing advanced technologies like Splunk, Nessus Tenable, and CrowdStrike for proactive threat detection and the protection of healthcare data. MDC's support in these efforts has led to substantial improvements in mitigations, diagnostics, and cybersecurity risk management—all of which are crucial for safeguarding public health.



Together, we can set new standards for data protection and resilience in the healthcare sector. Partner with MDC today and lead the change towards a more secure, health-centric digital future by reaching out to businessdevelopment@mdc-llc.com.