Demystifying data **analytics and protection**

Machine learning and cloud technology can help agencies become more efficient and secure

Rob Roy
Public Sector CTO, Micro Focus Government Solutions

MANY CYBERSECURITY BREACHES happen when an adversary takes over a legitimate identity. Therefore, a good network defense strategy relies on machine learning to monitor user behavior and make sense of data from billions of cybersecurity events, which is impossible for a human to do.

For example, anomalous user behavior is marked by a series of activities outside their normal behavior, such as a U.S. employee logging in at 3 a.m. from an IP address in China, accessing a database he's not supposed to have access to and downloading files to a local computer. A network administrator seeing those activities can conclude that a breach is in progress and shut that person off.

With unsupervised machine learning, agencies can start putting the onus on computers to recognize unusual behavior. Unlike the rules-based approach, unsupervised machine learning lets the technology develop an understanding of how the network's users typically behave and alert administrators when something abnormal occurs, increasing the likelihood that a rogue event is detected and a response is orchestrated at machine speed.

Letting computers do what they do best

Machine learning is rooted in analytics. There's no lack of data to analyze in the government, and in fact, most agencies have more data than they know what to do with. Understanding what to look for in all that raw information requires the help of data scientists, who can tell agencies how to solve a problem or answer a question by identifying the relevant data to analyze.

Then the technology can step in and do the repetitious and very rapid work that computers do well. The resulting analysis provides the insights that leaders need to make good decisions.

Throughout the process, agencies need to safeguard the data and comply with rules governing privacy. The government has a mandate to encrypt data when it's at rest, but data is vulnerable if it's not also encrypted while it's being used.

For example, if the information in a large agency database is unencrypted for use, hackers could mount a successful phishing campaign and take over a user's credentials. That could allow them to log in as a legitimate user and download the contents of the database. All that data is unencrypted, which means all the personally identifiable information is exposed. Therefore, it's important for the government to move to the next stage of protecting data in use.

Moving legacy systems to the cloud

When it comes to modernizing the government's approach to cybersecurity, legacy systems present some special

davooda/Shutterstock/FCW Staff

> Unsupervised machine learning lets the technology develop an understanding of how the network's users typically behave and alert administrators when **something abnormal occurs**.

challenges. Agencies still rely on a lot of mainframe capabilities that are costly to maintain. In addition, those mainframes run on COBOL, a very robust but very old language. The workforce that supports it is retiring from government, and new employees don't have experience with COBOL.

Those legacy systems run mission-critical government functions, so we need to find a way to secure them and make them cost-effective. Moving legacy systems to the cloud can reduce the annual maintenance cost of some systems by as much as 90 percent and can enable organizations to take advantage of innovative new technologies. For example, some commercial clouds have machine learning and analytics built in.

Micro Focus has developed technologies and capabilities that enable organizations to take a low-risk approach to moving their COBOL-based mainframe applications into the cloud. By modernizing in that way, agencies experience the same availability, the same or even better performance, and improved security. ■

Rob Roy is public sector CTO at Micro Focus Government Solutions.