Modern tactics for today's cyber battlefield

Agencies' IT systems have been built on a castle-and-moat defense model. But when it comes to safeguarding critical information assets, organizations must adapt to adversaries who are using guerilla tactics and no central command structure.

Putting threats into context

Advances in data analytics and user authentication bolster agencies' defenses

Mark Settle
CIO,
Okta

OUR TECHNOLOGY ARCHITECTURES have historically been designed to provide network-based defense in depth, which is becoming increasingly irrelevant. Network connectivity has become ubiquitous, there is no limit to the diversity of devices that can sit behind IP addresses, and threats no longer appear one at a time.

Practically speaking, advanced analytics is the only viable solution for coping with the vast amount of data that is routinely collected to monitor the movement of information across our networks, data centers and cloud-based systems.

Three emerging trends will enable us to extract context from this data in the future. Deep machine learning will play an increasingly important role in detecting anomalous patterns of system access and usage. Bots will crawl historical knowledge bases to match real-time anomalies — known or suspected — to similar events in the past. Finally, conventional predictive models that are based on snapshots of past conditions will be supplanted by streaming analytics, which is designed to ingest a far broader cross section of descriptive parameters and continually cull the mix that is most relevant for immediate detection and forecasting.

To further protect systems, identity authentication will not be a one-step process in the future. Rather, multiple challenges will be issued as end users attempt to access increasingly sensitive forms of information. Conventional hard tokens, software tokens with limited lifetimes and biometric tokens will play a key role.

We have to stop thinking about security vulnerabilities as static and start thinking about them in contextual terms that can change based on user identity, endpoint location, device, time of day or even current events. ■

Mark Settle *is CIO at Okta.*