Applying the OODA Loop to U.S. Air Force Cybersecurity

Speed is crucial to success in both air-to-air combat and modern cybersecurity

By **Ralph Kahn**
Vice President Federal
Tanium

In the middle of the Korean War, Air Force Colonel John Boyd noticed something odd: America's fighter pilots were winning a majority of aerial battles, even though the enemy's planes maneuvered far better than the American F-86 jets. But the American jets had two crucial advantages: a bubble canopy that gave pilots a near complete field of vision, and hydraulic controls that let pilots move faster and with more ease. These factors made all the difference.

Boyd broke down what was happening into four steps, a process he called the OODA Loop: observe, orient, decide, act. Whoever completed these steps faster would win the battle. Speed, in particular, is key—the faster a pilot moves through the OODA Loop, the faster they can disrupt and lengthen the enemy's own loop.

> Boyd broke down what was happening into four steps, a process he called the OODA Loop: observe, orient, decide, act. Whoever completed these steps faster would win the battle.

Since the 1950s, the OODA Loop has been applied more broadly to warfare theory and also to business strategy. In fact, all humans go through the OODA Loop hundreds of times a day — each time we make a decision, we observe our environment, orient ourselves by putting our observations into context and applying past experiences, make a decision based on that information, and then we act on it. This process often happens subconsciously and in milliseconds.

The OODA Loop can also be applied to cybersecurity. In fact, the process is an ideal fit for cybersecurity because of speed's importance — cyber attackers operate in seconds, and can cause exponentially more damage the longer they are inside a network. Cyber defenders must be faster. As Lieutenant General Bradford Shwedo, the Air Force's Chief Information Officer, said at a Trezza Media Group 2017 forum, "Speed is life — nothing is more true in cyber."

Today, the U.S. Air Force's cyber warriors are applying the same OODA Loop to protect its cyberspace that its fighter pilots were using in the air six decades ago — and Tanium is helping.

Together, we developed the Automated Remediation and Discovery Program (ARAD), which is helping the Air Force manage its 600,000 endpoints and complete the OODA Loop faster than its enemies. Here's how it works.

Step 1: Observe

Just as the American F-86 pilots flying over Korea benefitted immensely from a complete field of vision, the Air Force's cyber warriors need a complete view of every endpoint on their network. That can be a challenge when you have a massive IT environment, with laptops and mobile devices constantly coming onto and off the network. But not for the Air Force. Tanium is giving the organization complete visibility into each endpoint and its status in real time. This clear line of sight is the foundation for the next steps.

Step 2: Orient

The Air Force's network faces hundreds of thousands of attempted attacks each day, and must be able to understand what needs immediate attention and what can wait. Reducing this noise is one of the biggest challenges the airmen face. Tanium is helping the Air Force's cyber warriors rapidly filter and comprehend this vast amount of data, raising critical issues to their attention, while allowing lesser priorities to be handled within normal cyber operations cadence.

Step 3: Decide

Because the Air Force now has a holistic view of every endpoint on its network, and the right context for understanding what's happening on those endpoints, its cyber warriors can make much quicker, more informed decisions, in order . They also have more time to make these decisions, because Tanium is automatically handling many tasks the cyber warriors formerly had to do manually.

Step 4: Act

The ARAD program enables the Air Force to rapidly enact any decision they make, and be confident those actions were successful — whether that's implementing a critical patch across their entire network in just hours, uninstalling software in minutes if they discover a vulnerability, or hunting for indicators of compromise across their environment. And because multiple Cyber Operations groups have a single platform to manage IT, implement patches, and respond to and remediate incidents, they are able to function with more effectiveness and efficiency.

ARAD's impact

The Air Force's response to the WannaCry attack is illustrative of how ARAD has transformed the organization's security. ARAD rapidly scanned all 600,000 endpoints, patched the ones that needed patching, and quarantined systems that seemed suspicious.

Before, it would take weeks to understand which devices needed patching and then to implement those patches across each endpoint. Compliance audits were also a long, lethargic process requiring Air Force staff to manually search for vulnerabilities and patch each endpoint individually. Now, the Air Force is compliant with U.S. Cyber Command regulations every day, saving the organization significant time and money.

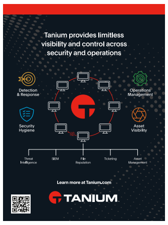
That reduced workload, combined with a much deeper visibility into their network, enables the Air Force's IT staff to tackle bigger technology challenges, like consolidating data centers and moving to the cloud.

With ARAD, the Air Force is continuously completing the OODA Loop — observing, orienting, deciding, and acting — all in seconds. The Air Force's ability to operate at the speed of cyber, both across its entire enterprise and surgically on an individual endpoint, is keeping them a step ahead of the enemy, and dramatically improving their security. ■

SOLUTION FOCUS

15-Second Visibility and Control Over Every Endpoint. Even Across the Largest Networks.

Tanium gives the world's largest enterprises and government organizations the unique power to secure, control and manage millions of endpoints across the enterprise within seconds. Serving as the "central nervous system" for enterprises, Tanium empowers security and IT operations teams to ask questions about the state of every endpoint across the enterprise in plain English, retrieve data on their current state and execute change as necessary, all within seconds.



With the unprecedented speed, scale and simplicity of Tanium, organizations now have complete and accurate information on the state of endpoints at all times to more effectively protect against modern day threats and realize new levels of cost efficiency in IT operations.

In a fully digital world, the lifeblood of an organization lies in its ability to gain the upper hand against bad actors by moving faster than they do and stopping attacks before they cause irreparable damage. The rising number of security breaches across both the public and private sectors is directly caused by IT's inability to find or fix the issue quickly enough at scale — the incumbent approaches and tools are too slow and scale too poorly to secure and manage the rising number of business-critical IT assets today.

Tanium is fundamentally transforming IT with the industry's only platform capable of delivering 15-second visibility and control over millions of geographically distributed endpoints, from laptops to desktops to virtual machines to cloud assets to ATMs.

Instead of relying on data that is hours, days or weeks old, security and IT operations teams now have accurate and complete data that is only seconds old and the unique ability to make changes across the enterprise in seconds as well.

With authoritative data on what is actually happening — as it's happening — and the ability to make change nearly immediately, organizations are now back in the driver's seat to stay ahead of attackers and reclaim operational inefficiencies that have plagued them for years.

Visit us at www.tanium.com or follow us on Twitter at @Tanium