PLURALSIGHT

MeriTalk

Training, Upskilling Are Key to Fighting Cyber Threats

As Federal agencies ramp up their defenses against potential cyberattacks, the threat landscape grows ever more worrisome. Nation-state actors are using cyber threats to soften the ground for physical attacks, steal secrets, and impose economic costs on America. Targets include Federal agencies such as the Department of Energy, which governs the energy sector, defense agencies, and critical infrastructure.

Federal investigators are especially concerned about critical infrastructure and the escalating threat from China. The U.S. Government Accountability Office says risks to critical infrastructure nationwide are increasing, an assessment reinforced by a cybersecurity advisory in February from multiple Federal agencies. It warned that Volt Typhoon, a Chinese state-sponsored hacking group, is seeking to pre-position itself on IT networks for potential cyberattacks against critical infrastructure in the event of a major crisis or conflict with the United States – and has already compromised the IT environments of multiple U.S. critical infrastructure organizations.

The Federal Cyber Response

In response to the spiraling threats, Federal agencies have rapidly expanded their cybersecurity capabilities, guided in part by the White House's 2023 National Cybersecurity Strategy. An overarching theme of cyber response is zero trust, with agencies working to meet a Sept. 30, 2024 Office of Management and Budget deadline for specific zero trust standards and objectives.

To accelerate progress, agencies are implementing controls in their environments, identifying gaps, and translating zero trust requirements to existing controls. Agency network engineers, for example, may be close to meeting zero trust requirements – and will be able to identify specific areas that need attention once the relevant technical controls are mapped to zero trust standards.

The Cyber Skills Challenge

For many agencies, the biggest challenge in the national cyber response is the ability to translate cyber mandates into hands-on keyboard activities. Ultimately, cybersecurity is not a technology problem; it is a people problem. The reality is that cyber attackers are humans on the other side of computers. That means those on the government side must be better-trained humans who can extract a greater cost on the enemy in response.

Recent MeriTalk research, in partnership with Pluralsight, found that of 150 Federal cybersecurity leaders surveyed, 61 percent said agencies should build their cyber capabilities by enhancing recruitment and retention of highly skilled cybersecurity professionals.

But recruitment alone won't solve the cybersecurity skills problem. Ninety-two percent of cybersecurity professionals say their organization suffers from skills gaps in one or more areas, and 43 percent cite one or more significant or critical skills gaps, according to the 2023 ISC2 Cybersecurity Workforce Study, a survey of

14,865 cybersecurity professionals globally. Importantly, 58 percent of respondents to the ISC2 survey said the negative impact of worker shortages can be mitigated by filling key skills gaps.

Experts say the cyber skills gap stems from a number of factors, including the tendency of traditional computer science degree programs to prepare students for governance and compliance jobs, rather than hands-on-keyboard roles. And with technology advancing, professionals must continually learn to keep up and advance. Yet studies show that while many cybersecurity professionals seek at least 40 hours of training each year, nearly a quarter don't meet that goal.

The Pluralsight Approach

Pluralsight makes the most of available training time by meeting students where they are on their educational journeys, from beginners just learning their jobs to advanced security experts who may just need a 30-minute hands-on lab.

At all levels, courses are conducted by trainers with deep Federal technical expertise – and align with mandates and the White House's National Cyber Workforce and Education Strategy and the Department of Defense (DoD) Cyber Workforce Framework (DCWF).

Because finding the time to study is a challenge for busy security professionals, Pluralsight utilizes the just-in-time learning approach – get the information you need right when you need it, and if you need to study one topic, don't sit through an entire course.

In other words, work smarter, not harder.

Pluralsight Security Courses and Paths

Pluralsight puts this guiding principle into action with a wide variety of courses, hands-on labs, and learning paths to help agencies upskill their workforces and fulfill zero trust requirements. To determine where students are on their learning trajectories and put them on the fastest path to learning, Pluralsight offers short skills assessments.

Pluralsight's offerings include:

- Security Breaking News, a tailored learning path covering critical new vulnerabilities in Federal systems, how attackers have tried to exploit them, and how employees can identify threats. The path focuses on zero trust-related themes such as firewall control, network access control, and limiting internal network movement
- Security Hot Takes, a course that examines new topics in the cybersecurity realm such as the introduction of generative artificial intelligence at Federal agencies. Security Hot Takes also addresses subjects such as breaches of Federal systems and potential software weaknesses in those systems
- Critical Vulnerabilities and Exploits (CVE), hands-on labs that teach participants how to find common CVEs and protect against them
- Security Hands-On Sandboxes, a learning path that provides hands-on experience in detecting and responding to network and endpoint attacks
- An upcoming learning path addressing Volt Typhoon, detailing the threat and providing a lab in which students can emulate attacks in order to stop them

A Trusted Federal Partner

Pluralsight's workforce development platform helps Federal agencies advance cybersecurity goals through mission-critical skills, process improvements, and data insights. Develop the best defense by developing your people first.

To learn more, visit
pluralsight.com/industries/public-sector