WHY AUTOMATION TOOLS ARE KEY TO ENHANCING DOD'S DIGITAL WORKFORCE

FedScoop Report

The military's push to advance cloud, C3, AI and cybersecurity capabilities — and get contractors CMMC-certified — call for powerful IT automation platforms.

High-performing organizations, and those who lead them, have learned the importance of maintaining operational excellence and resiliency even when their personnel turn over constantly. And no organization has learned that better than the U.S. military.

The continuous rotation of officers and enlisted personnel to new assignments across the globe remains a vital part of maintaining military readiness. Sustaining that readiness, though, requires a massive commitment to underlying support systems and constant training at a scale that's hard for most enterprises to fathom.

Technology, of course, plays a fundamental role in those support systems. However, the natural churn in personnel responsible for maintaining and protecting the IT systems that support the U.S. armed forces around the world creates a special challenge for military leaders.

That challenge has grown more urgent as Defense Department officials place increased strategic importance on digital modernization, as part of the ***National Defense Strategy***. Central to the success of that strategy is the need to mobilize greater attention around five critical areas — data, cloud, artificial intelligence, C3 (command, control, communications) and cybersecurity.

That in turn requires building and retaining the right skills, experience and institutional knowledge to ensure that thousands of existing IT systems around the world — and new ones still being established — are operating and maintained properly at today's military tempo.

Power of automation

Fortunately, advanced IT tools — that can automate daily software, infrastructure and security maintenance routines — now make it possible for the military to take a more productive approach in how they train, manage and support their IT and communications personnel.

Security orchestration, automation and response (SOAR) tools, such as Splunk's Phantom platform, provide the means for instance, to monitor a wide range of existing technology systems and applications; identify their health in real time; and apply prescribed remedies all in an orchestrated, automated and controlled approach. Rather than having to chase down alerts, respond to sudden abnormalities or deploy routine updates on various systems, military IT personnel can focus more of their time and attention on modernizing and enhancing their unit's cloud, AI, C3 and cybersecurity platforms.

Moreover, by automating many of today's routine IT and security tasks, the military can reduce operating costs as well as IT risks that inevitably occur during handoffs as personnel rotate in and out of position, according to Eric Hennessey, staff consulting solutions engineer for national defense accounts at Splunk.

"Automation not only helps preserve the institutional knowledge often lost when technical personnel leave for new assignments," he said. "It also helps streamline orientation and training when new personnel take over, allowing them to get up to speed faster and focus on more critical tasks."

> ***Automation not only helps preserve the institutional knowledge often lost when technical personnel leave for new assignments. It also helps streamline orientation and training when new personnel take over.***
>
> ***– Eric Hennessey, Splunk***

Rising IT stakes for DOD

The scale, scope and velocity of those tasks are clearly intensifying as the military looks to provide greater digital support for roughly 1.34 million soldiers, sailors, Marines and airmen/airwomen, and another 775,000 active duty civilians, operating at hundreds of bases and facilities around the world. That's not to mention another 800,000 men and women in the reserves, according to recent ***Defense Department figures***.

One measure of the Defense Department's IT workload is reflected in the department's latest available ***Fiscal Year 2021 budget request*** for Information Technology / Cyberspace Activities. The budget calls for $37.7 billion in unclassified IT investments and expenses and another $11.8 billion in classified IT spending. And that level of annual IT investment spending is projected to continue at least through 2025.

A deeper dive into the numbers shows $14.8 billion in classified and unclassified IT spending going to the Army; $11.0 billion to the Navy/Marines; $8.2 billion to the Air Force; and $15.9 billion to Defense-wide projects. Nearly $10 billion of those funds are slated for cybersecurity and the cyberspace domain projects, including next-generation encryption solutions and network modernization.

All of that IT spending reflects the growing need to acquire, manage, maintain and remediate more modern technology systems on a scale that makes the use of automated, AI-assisted operating platforms essential.

Consider how automating IT routines could streamline support activities, for instance, at the Defense Logistics Agency alone, which employs about 25,000 civilians, 500 military and 4,000 contractor personnel, operates a global network of distribution centers, and provides more than $35 billion in goods and services annually.

Automation is poised to play an even wider role in managing IT and data analytics systems that support military engagements.

"The period of 2020–2040 seems likely to see even more change in the technologies and the character of warfare than have recent decades," suggest military experts Michael E. O'Hanlon and James N. Miller in a ***Brookings Institution essay***. Fast-moving changes in "various aspects of computers and robotics…will be joined by various breakthroughs in artificial intelligence and the use of big data," along with robotic systems usable as both sensors and weapons.

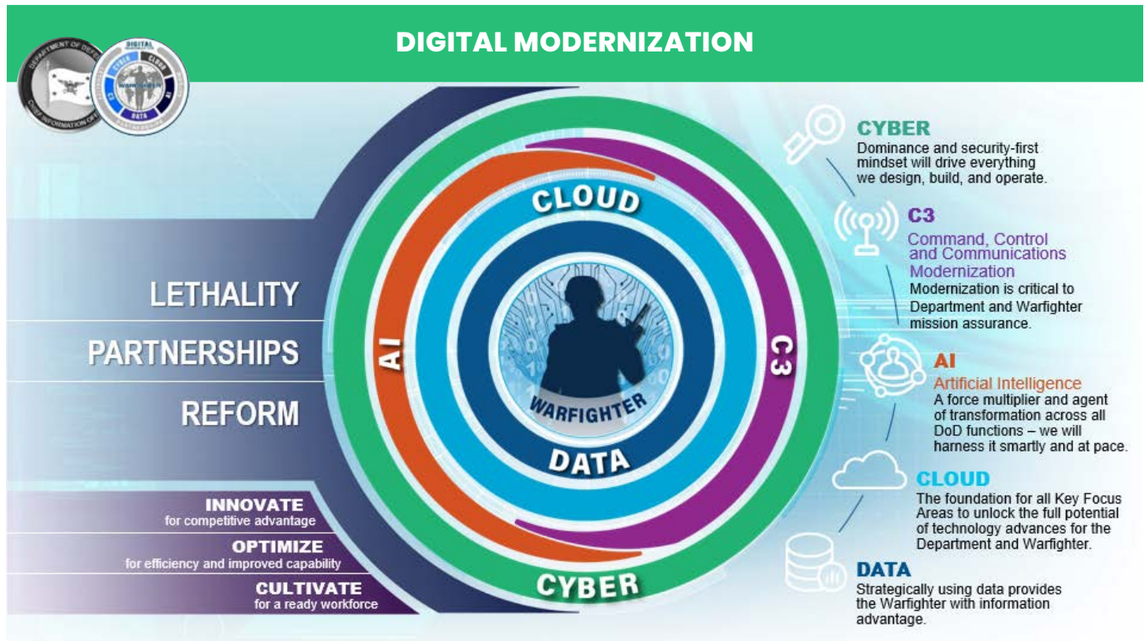
"The key question will be how these technology trends interact synergistically with each other, and how military organizations as well as political leaders innovate to employ them on the battlefield," they said.

Augmenting IT workloads

"One area where automation tools can really help is in institutionalizing repeatable processes," said Hennessey. "Because people are constantly coming and going, user accounts have to be constantly created and removed. Those types of processes are pretty straightforward and repeatable and very easy to automate. By taking that workload off the service desk staff, they can concentrate on other more important things."

Another benefit of automation is the collective reduction in problems or delays that arise from gaps in continuity and expertise as IT personnel rotate in and out, which creates additional work.

Perhaps the biggest benefit of automation, though, "is removing the error factor," he said. "Whenever you can take humans out of the loop on some of these repetitive tasks — and institutionalize repetitive processes, using an automated playbook like we do with Phantom, you greatly reduce that opportunity for error."



Read the DoD Digital Modernisation Strategy at https://dodcio.defense.gov/

Source: DoD Budget Overview

Expanding orchestration and automation

Splunk Phantom, he explained, gives network operations teams an open and extensible automation platform that provides multiple interfaces to some of the most commonly used IT and security products out on the market. It combines security infrastructure orchestration, playbook automation and case management capabilities to integrate processes, security workflows and other tasks.

"So if I need to be able to sign into a switch port on a network security device in response to an event, Phantom can automatically go there and lock down that port from being able to communicate with the rest of the network in response to a threat," he said as an example.

IT teams can codify workflows into automated playbooks, using a visual editor, so no coding is required, reducing training requirements as well as time spent executing repetitive tasks.

But perhaps even more importantly, Phantom helps security teams detect, investigate and respond to threats at machine speed, reducing malware dwell time, and lowering overall meantime to resolve incidents, saving IT workforces significant amounts of time and resources.

Phantom's dashboards actually can equate those activities into time and budget dollars saved, to help IT teams demonstrate where a SOAR system is making a difference, according to Hennessey.

And with services like ***Splunk On-Call***, developers and operations teams can mobilize quickly and collaborate intelligently to resolve incidents and reduce downtime quickly, using context-rich notifications.

"Phantom can take data feeds from anything," in ways that will be familiar to users of Splunk's broader "Data-to-Everything Platform" solutions, he added. Splunk's automation and analytics capabilities are already widely in use across the military, analyzing everything from aircraft diagnostics data, to ship maintenance records, to weapons performance logs. That analysis in turn is being used to help predict when parts need to be replaced, or when system failures appear imminent.

Supporting CMMC practices

Automating IT processes is also about to take on much greater importance for defense contractors, who must now meet the Pentagon's Cybersecurity Maturity Model Certification (CMMC) audit and accreditation process, ***according to Anthony Perez***, Splunk's Global Solutions Architect.

To ***achieve certification***, DOD contractors will need to deploy and adopt proven enterprise-grade technology that can be iteratively tailored and extended to prove they can meet the unique demands of the CMMC criteria. That will mean establishing repeatable, integrated processes that streamline monitoring, execution and audit preparation. But it will ultimately require the ability to collect and monitor data from vast collections of sensors, applications and other sources — spanning a whole variety of siloed tools and digital formats — all at high volumes and velocity.

"From the contractor perspective, I envision organizations leveraging [Splunk's automation tools] to automate the self-evaluation of their cyber security maturity, identification of gaps, and generation of the bulk of their technical evidentiary package for C3PAO [third-party] auditors to use in their evaluation and CMMC-audit and accreditation process," says Perez.

From the military's perspective, that kind of IT workforce automation will prove both fundamental and essential in the march to digital modernization and data-driven readiness.

Find out more on how Splunk Phantom can accelerate the performance of your IT workforce.

This article was produced by FedScoop and underwritten by Splunk.

FEDSCOOP

splunk>®