BREAKING DEFENSE

SPOTLIGHT:

Automate the Complex: Network Automation Enables Military Interoperability and Agility

Sponsored by

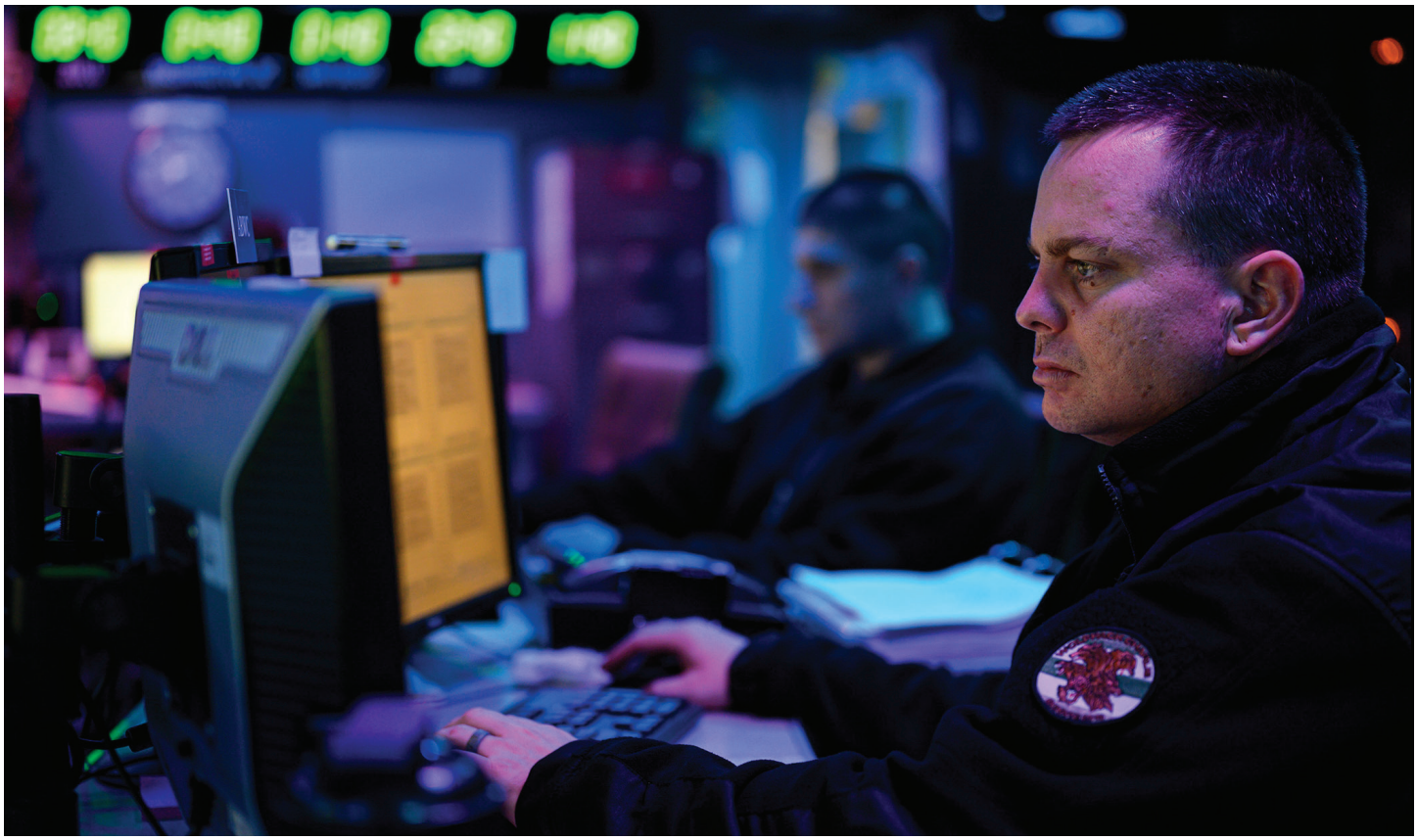
Red Hat

AUTOMATE THE COMPLEX:

Network Automation Enables Military Interoperability and Agility

BY BARRY ROSENBERG, Contributing Editor, Technology & Special Projects

Network automation is a key enabler that lets Special Operations Command fight both terrorists and peer/near-peer competitors in the Great Power competition.



Network automation employs AI/ML and analytics to augment or replace human intervention in the identification and containment of cyberattacks.Shown is the Joint Operations Center aboard amphibious assault ship USS Boxer during exercise Eager Lion in 2019.

The reality of military networks today is that there are, perhaps, too many of them. There are enterprise networks and tactical networks, Army, Navy, Air Force, and Marine Corps networks. Each operates at multiple security classification levels via the Non-classified Internet Protocol Router Network (NIPRNet), the Secret Internet Protocol Router Network (SIPRNet), and the Joint Worldwide Intelligence Communications System (JWICS).

There have been efforts over the years to collapse and consolidate networks so that military services can securely share data across branches and collaborate more efficiently with allies. Such integration is a key goal of the concept of Joint All Domain Command and Control (JADC2), which will help the Defense Department transition from the fight against violent extremist organizations (VEOs) to peer and near-peer competitors like China and Russia.

That challenge is particularly acute for organizations like U.S. Special Operations Command (SOCOM). While counter-VEO remains its top priority, SOCOM is working to rebalance its operations toward Great Power competitors—especially as these competitor powers have been known to employ VEOs, whether witting or unwitting, as proxies.

One of the key tools that SOCOM is using to rebalance its mission is network automation. Like all of DoD, SOCOM is experiencing a surge in cyberattacks, so analysts working in its information security operations centers (SOCs) are being bombarded with security alerts from their security information and event management (SIEM) systems. With so many such events, it's hard for them to differentiate true alerts from false ones, and to determine which events are priorities to address immediately. Through no fault of their own, they end up wasting time in basic functions that could be better spent on mission-critical and higher-end analytical activities that directly support warfighters.

"There's a phrase I use a lot; we need processes that serve us as opposed to us serving processes," said Lisa Costa, chief information officer and director of command, control, communications, computers at SOCOM, speaking recently during a Breaking Defense webcast.

"The way to fundamentally get after network automation capabilities is to look at what are those pain points that are causing us to spend numerous hours of touch labor? I'll tell you, that really kills us. Touch labor per device is something that is incredibly challenging when you run a distributed network.

"An example of where we're automating is using Ansible," said Costa, referring to the open-source software that enables the use of Infrastructure as Code (IaD) for configuration management and application deployment, and which was acquired by Red Hat in 2015. "We've used it to develop automated playbooks to develop servers, to push patches, and to cut the amount of time needed to develop data center servers from two weeks to a matter of a few minutes. That's time that adds up when you're having to build 60-200 servers. We're definitely focused on automating the pain points of that touch labor. Being able to put this into a reusable playbook has been life-changing for us."

Automation Reduces Cyberattack Severity

Network automation employs technologies such as artificial intelligence, machine learning, analytics, and automated orchestration to augment or replace human intervention in the identification and containment of cyberattacks. IBM quantified the importance of network automation—and the bottom-line costs to organizations, both civil and military—in its Security Cost of a Data Breach Report 2020, produced with the Ponemon Institute.

Data breaches caused by malicious attacks are the most common and costly to organizations and are growing in numbers, states the report. The worst threat vectors are stolen or compromised credentials and misconfigured cloud servers. These two tie for the worst—i.e., the most costly—causes of malicious breaches.

The average time it takes to identify and contain a data breach, what's known as the breach lifecycle, totaled 280 days in 2020. Speed of containment can significantly impact the damage done and breach costs, which can linger for years after the incident.

This is where network automation comes in. From detection to containment, the IBM study shows that the financial cost of breaches—a top concern for both industry and DoD—directly relates to whether an organization used automation tools such as AI and implemented incident response (IR) preparedness, including formation of IR teams and testing of IR plans. Those that did experienced significantly lower costs to remediate the attack.

Lisa Costa, chief information officer and director of command, control, communications, computers at SOCOM.

Organizations that did not deploy security automation were out of pocket an average of $6.03 million, more than double the $2.45 million out-of-pocket cost for those that did.

Savings in average total cost of a data breach in organizations that established an IR team that proactively tested its plans brought the response cost down even more.

Those eye-opening figures are for just a single breach, which explains the significant growth in the number of organizations turning to automation, says IBM. The percentage of businesses with fully deployed security automation, defined as the use of artificial intelligence platforms and automated breach orchestration, grew from just 15 percent in 2018 to 21 percent in 2020, study reports.

Automation and CI/CD

Already a tool for network management and cyber-incident response, automation also plays an important role in development of new software applications through the use

of Infrastructure as Code and the process of continuous improvement/continuous delivery (CI/CD). Better known as agile software development, DevOps, or DevSecOps (when cybersecurity is part of the process), CI/CD embraces an iterative process: develop minimally viable software, get user feedback, develop a little more, and repeat.

Automation is already playing an important role in bringing DevSecOps to the network arena as it codifies the steps, procedures, and processes necessary to implement specific networking objectives. That lets the automation framework be version controlled so that when similar tasks need to be repeated they can be exactly replicated by leveraging automation playbooks or procedures. With this capability, less experienced network administrators can execute more sophisticated network configuration.

Kevin Griffith, senior director responsible for DoD program outreach at Red Hat.

"By bringing DevSecOps practices and automation to network configuration activities, we are able to better position the enterprise to implement digital transformation," said Kevin Griffith, senior director responsible for DoD program outreach at Red Hat. "Embracing disruption and change is necessary to gain the benefits of digital transformation. Changes that need to cascade across a network domain can be easily replicated and modified in totality.

"Perhaps even more valuable than quick modifications is the ability to easily revert configuration changes. This ensures that in the event of a misconfiguration, returning to a known working state is much quicker."

For SOCOM, which runs the fourth largest IT enterprise in the DoD supporting 80,000+ users, automation for software development is part of its priority to "operationalize innovation." Agile Dagger, as SOCOM's agile software development program is called—complementing other DoD programs like the Air Force's Kessel Run project—is one DoD element in a convergence of technologies needed to address the Great Power competition, others being 5G and artificial intelligence/machine learning (AI/ML). This stands in contrast to point technologies such as full-motion video targeted at the terrorist threat.

"You have to fundamentally change the way that software is acquired in order to be able to continuously deliver it and continuously improve it," said Costa. "We're operationalizing AI and ML so analysts can focus on the signal rather than on the noise. This is where our CI/CD pipeline really is important, because instead of having to deliver an entire stack of software we can deliver microservices that monitor a sensor feed, for example, and determine when something important has happened, and then transmit that information."

Costa added that one of the goals of the Agile Dagger software development pipeline is to put a new spin on the agile mantra known as "fail fast."

"We've all heard the term 'fail fast,' which came from the venture capital and start-up arena," she said. "Well, when you have only invested a little bit in something it's easy to fail fast. But if you're invested in a five-year program with requirements documents, requests for information, and a request for proposal, followed by two or three years to get a capability back, let me tell you, nobody wants to hear that you failed. So where we're trying to go with DevSecOps is to be able to fail fast but do it in a controlled and responsible manner."

Automate the Complexity

The DoD's increasingly complex security environment is defined by rapid technological change and challenges from adversaries in every operating domain. "In this environment, there can be no complacency—we must make difficult choices and prioritize what is most important," the most recent National Defense Strategy states.

As Costa mentioned, network automation is one of those prioritized capabilities. For the security analysts on the front lines of incident management, automation reduces errors and maximizes skills by letting them focus on solving problems. It is also a key enabler to facilitate collaboration across networks and streamlines the ability of software developers to deliver better applications in accelerated timeframes.