Enhance cyber resilience in global defense

"Defense organizations must navigate these obstacles by adopting a unified platform approach, using an open framework based on open standards to strengthen autonomy, security, and consistent operations across all environments."[1]

Giuseppe Magnotta
Associate Principal Solution Architect, Red Hat, EMEA

Achieve cyber-resilience action plans for defense stability

Cyber resilience forms the bedrock of continuous operational readiness for defense organizations across the globe. To effectively operate in and through contested and congested cyberspace, defense forces require the following core capabilities:

- **Maneuverability.** Defense cyber operators must possess the capability to rapidly restore destroyed or degraded applications in various global locations—whether in public clouds, base datacenters, or at the tactical edge (e.g., aircraft, ships, vehicles, and portable fly-away kits deployed internationally).
- **Interoperability, for unity of effort and multicapable forces.** Each defense service component, irrespective of its geographic location, utilizes servers and network devices from multiple vendors. In multidomain operations (MDO), cyber operators need the ability to manage any vendor's device without requiring knowledge of vendor-specific commands for software updates, configuration changes, capacity additions, and other actions vital for global resilience.
- **Rapid application deployment and scaling.** Science developer teams within defense agencies globally continually retrain and tune AI and machine learning (AI/ML) models and applications used for offensive and defensive cyber operations and decision dominance. Resilience against new threats necessitates the ability to rapidly scale capacity for model training and to deploy new models in the location closest to warfighters, without requiring specific training on the hardware in that particular region.
- **Visibility across the cyber terrain.** Operators need strong visibility into the cyber terrain to effectively identify the source of new threats and deploy effective countermeasures across their global networks.

Accelerate cyber resilience with Red Hat technologies

Defense organizations worldwide can significantly accelerate their cyber resilience initiatives by using Red Hat® technologies for automation and interoperability.

Red Hat Ansible® Automation Platform automates recovery of destroyed or degraded capabilities at mission speed. This means cyber operators do not need to learn vendor-specific commands to configure, deploy, and scale services as the platform translates natural language intent (e.g., "add a new route") into the appropriate commands for each device, simplifying global operations.

A hybrid cloud application platform powered by Kubernetes, Red Hat OpenShift® accelerates resilience by allowing containerized applications and virtual machines (VMs) to be moved to different vendors' server hardware in any location, with little or no modification. For example, if a base datacenter is destroyed in one country, its applications can be restored to a public cloud in

1 *Red Hat blog. "From core to tactical edge: A unified platform for defense innovation," 25 Aug. 2025.*

another region, and vice versa. Workloads can also run on small, resource-constrained devices at the tactical edge (e.g., aircraft, vehicles, ships, and portable fly-away kits) running Red Hat Device Edge. Devices running on Red Hat Device Edge can effectively operate in Denied, Disrupted, Intermittent, and Limited (DDIL) network conditions, continuing to collect and analyze data even when a connection is not available in remote or challenging environments.

Benefits of working with Red Hat:

- Rapid application deployment and scaling with a unified platform
- Increased visibility across the entire cyber terrain
- Flexibility to automatically execute playbooks or transition workloads

Use cases for cyber resilience field work

Automate maneuverability

Mission challenge: When a primary defense site is under attack, traditional manual failover to a secondary or tertiary site can take an hour or more, severely threatening mission survivability across global operations.

How Red Hat can help: By detecting an event that puts the mission at risk, Ansible Automation Platform automatically executes a playbook of predefined actions to confront the risk in near real time. If the primary site is inoperable, Ansible Automation Platform and Red Hat OpenShift work together to automatically transition mission-critical workloads to a secondary site or recovery point, which might be a base, public cloud, or edge server anywhere in the world. No human intervention is needed. Instead, the Event-Driven Ansible feature monitors for conditions such as failure of communications lines or servers, and then executes automated actions to reconstitute services from the alternate location (Table 1). Red Hat OpenShift makes certain that business-critical applications operate consistently regardless of their deployment location. Mature, automated workflows support goals for continuity of operations (COOP) for global defense.

Table 1. Examples of adverse events recognized and remediated by Ansible Automation Platform

Threat	Sample playbook response
Failed communications line	Transition workloads to an alternate site
Malware discovery	Take the infected system offline while activating a new one in real time, scale application services up or down, or close a firewall port
Cluster node stops responding	Reconstitute workloads on another node
Configuration deviations on the VM or container, causing a security vulnerability	Identify and execute self-healing actions

Unify efforts across the cyber terrain

Mission challenge: Each defense service component, globally, uses servers and networking devices from many original equipment manufacturers (OEMs), each with its own management tools, operating systems, and commands. Even within a single department, cyber operators need extensive training on various toolsets to manage deployments effectively.

How Red Hat can help: With Red Hat OpenShift, applications can be built once and then deployed anywhere from the hybrid cloud to the edge. This means that ML models and AI-based applications developed by a single department or component can be deployed on any other department's or

component's servers, promoting unity of effort and a multicapable IT workforce across international defense collaborations. Automation, through Ansible Automation Platform, further contributes to unity of effort because IT specialists in each department can work toward a common operational capability without learning specific technology commands for each of many IT systems. Ansible Automation Platform can automate actions that can be initiated from a command-line interface (CLI) or application programming interface (API).

Build and deploy warfighting capabilities rapidly, at scale

Mission challenge: Defense software teams continually add software capabilities, harden security, and tune ML models in response to evolving stresses and attacks. Software update cycles are often delayed because each domain uses multiple hardware platforms, some operating in DDIL environments across different nations. To accelerate cyber resilience, service components need the ability to deploy new and updated applications to disparate endpoints more rapidly, at scale, and with confidence that the applications will behave consistently on every platform.

How Red Hat can help: With Red Hat OpenShift, joint operations teams can build applications once and then deploy them to any environment of choice, from the datacenter or cloud to the mission edge. VMs can run alongside containers on the same node, which simplifies operations and maximizes resource use. When confronted by threats or adverse conditions, forces can autoscale capacity at the time of need, globally.

Joint operations teams can deploy standardized AI capabilities in geographically constrained areas by using Red Hat OpenShift, Ansible Automation Platform, and Red Hat Device Edge in combination. Consider a forward operating base (FOB) in a remote region that needs to update an ML model that captures and characterizes drone imagery. With Red Hat Device Edge, military platforms with unmanned aerial systems can be equipped with advanced software that lets small platforms handle large AI workloads, move with increased flexibility, and implement data-influenced decision-making in the field. Ansible Automation Platform allows operators to run a playbook to simultaneously deploy updated models to large numbers of drones or other edge devices. The effect is to accelerate mission outcomes by reducing errors, improving operational consistency, and adjusting to real-world threat information and mission needs with increased speed across global operations.

Streamline visibility and observability

Mission challenge: A defense agency is working to streamline compliance processes, reduce risk, and automate critical task deployment, patch and configuration management, and incident response. Barriers to success include the cyber exposure caused by massive surface attacks, ongoing changes to the security environment, and rapidly changing technology.

How Red Hat can help: Ansible Automation Platform provides a comprehensive inventory of the IT estate, allowing visibility across the cyber terrain (hybrid cloud, on-premise, and at the network edge). An accurate, up-to-date inventory helps IT teams accelerate resilience by scaling more quickly, reducing compliance risks, and swiftly identifying threats to availability so that they can be remediated.

To observe real-time events across the cyber terrain, use Event-Driven Ansible, included with Ansible Automation Platform. Event-driven Ansible constantly looks for specified events, automatically invoking predefined actions when an event is detected, providing business-critical situational awareness for global defense operations.

Learn more about resilience, automation, and interoperability

To remain a global leader, defense forces need superior capabilities. Learn more about ways Red Hat supports defense agencies to anticipate, withstand, and recover from the demands of adverse threat conditions.

Talk to a Red Hatter for more information or to get started.

About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with award-winning support, training, and consulting services.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#3094957_1225