Self-healing defensive cyber operations with CORA

Reference guide

Cyber Defense Posture

"Ultimately, the assessment provides commanders and directors a more precise understanding of their high-priority cyber terrain and their overall cyber security and defensive posture enabling greater command and control and enhancing decision making."[1]

Air Force Lt. Gen. Robert Skinner
HJFHQ-DODIN Commander

Infrastructure as Code (IaC)

Managing and provisioning of infrastructure through code instead of through manual processes.

Policy as Code (PaC)

Writing operational policies into automation code, so that internal requirements, security needs, and granular mandates are built into every process.

The challenge

Cyber warfare faces new challenges because of the fast-changing, competitive global landscape. Along with the changing character of war, cyber defenders are presented with significant new challenges. Offensive and defensive cyber operations have become more sophisticated, architectures are more complicated, and integrations are more prevalent—with data sharing across mission forces, agencies, allies, and coalition forces. This has resulted in an explosion of complexity across the Department of Defense Information Network (DoDIN) within enterprise and tactical environments that has increased the breadth and depth of attack surfaces available to innovative adversaries. In response to this evolution, Joint Force Headquarters, DoDIN (JFHQ-DoDIN), has introduced the Cyber Operational Readiness Assessment (CORA) to replace the Command Cyber Readiness Inspection (CCRI) process.

The CORA framework combats the increasing sophistication of adversarial activities and the growing complexity of DoDIN systems, by moving away from traditional perimeter based network security with periodic audits to a robust, proactive, continuously monitored, event-driven framework to protect the cyber terrain and maintain decision advantage to pace the threat through increased operational readiness, resilience, and robustness.

The doctrine

The CORA framework aims to achieve 3 key outcomes:

- Harden Information Systems
- Reduce attack surfaces
- Enable defense

The vital activities in defensive cyber operations are to detect, protect, and defend. To detect cyber attacks, exploits, and vulnerabilities, cyber assets must have instrumentation across the cyber terrain to collect vital telemetry. To protect cyber assets, cyber terrain visibility must provide active, real-time monitoring and alerting. To defend the cyber terrain, event-driven automation must be in place to remediate issues at the speed of relevance.

The CORA assessment process relies on tactics, techniques, and procedures (TTPs) from the MITRE ATT&CK framework to inform commanders and directors with a holistic vision of their cyber terrain and their cyber posture. This allows commands to prioritize their limited resources in the most critical areas of their cyber terrain to ensure readiness and protect the high-risk areas of information systems.

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

[1] *U.S. Department of Defense Spotlight. "JFHQ-DODIN Officially Launches its New Cyber Operational Readiness Assessment Program." 1 March 2024.*

The solution

The Red Hat® portfolio is widely implemented across the DoDIN and contributes important telemetry and capabilities to this effort, providing CORA assessors an operational picture of an IT estate's activity and operational readiness and resilience. This allows operators to harden their systems, reduce their attack surfaces, and provide a more proactive defense.

To ensure continuous operational readiness for warfighting systems, CORA uses behavioral and process patterns to gauge readiness levels, an approach that complements other components of the cybersecurity guidance library such as those that define zero trust for the DoD.

Zero trust architectures describe what and where (within the network and systems boundaries) to produce hardened information systems, and how to reduce attack surfaces by identifying protected surfaces and to provide a stronger defense by enforcing policies like least privilege access.

Harden information systems

The modern peer and near-peer adversary battlespace must rely on significantly more sophisticated information systems to coordinate activities in real time to support cross domain, intra-agency, and coalition forces. This move from data silos to data sharing to develop actionable intelligence presents new challenges that the traditional point-in-time surveys and actions of the CCRI process are inadequate to sustain. Hardening these dynamic, integrated, distributed information systems today across agencies and allies requires a shift to a multilayered, ongoing assessment and readiness approach that CORA provides.

Successfully inventorying and surveying the cyber terrain of these sophisticated information systems must rely on automation, Infrastructure as Code (IaC), and repeatable, scalable cloud-first architectures. This vital process allows the agility to respond and pace the threat. Monitoring of these systems requires a continuous interrogation of the IT estate. As the integrations and cooperating systems become more complex, the reliance on automation becomes more critical.

Reduce attack surfaces

It is common to consider the hardening of systems as synonymous with the reduction of attack surfaces. With the introduction of the Zero Trust framework and the rapid evolution of advanced adversaries, this outcome has evolved to include the reduction or removal of unnecessary technology from systems, and the elimination of implicit trusts throughout the entire services and data delivery chain—between producers and consumers of data.

Ensuring compliance with traditional security controls is important, but refining the very nature of systems architectures is necessary to effectively reduce the exploited attack surfaces, which extend from low-level hardware vulnerabilities up through sophisticated protocol and application-based attacks. Thus, the DoD has refocussed on data as the core asset to defend and protect, forcing their defenders to shift their perspectives towards a granular understanding and visibility of both the cyber terrain and active threat campaigns.

Configuration drift

The gradual divergence of a system's configuration from its intended or documented state.

Event-driven automation

The process of responding automatically to changing conditions in an IT environment, to help resolve issues faster and reduce routine, repetitive tasks.

Zero Trust architecture

A philosophy and architectural approach to the design and implementation of IT systems to eliminate implicit trusts to prevent data breaches and limit internal lateral movement.

Software development lifecycle (SDLC)

The process of developing software that is reliable, and trustworthy, enforcing security and visibility throughout the entire development lifecycle.

Software bill of materials (SBOMs)

A comprehensive inventory of all the components, including libraries, modules, and dependencies, that make up a software application.

Red Hat Enterprise Linux

A fully supported production ready, enterprise Linux operating system available on-premise, in public clouds, or on the mission edge.

Red Hat Ansible Automation Platform

A unified solution for strategic automation, combining the security, features, integrations, and flexibility needed to scale automation across domains, orchestrate essential workflows, and optimize IT operations.

Red Hat OpenShift Container Platform

A comprehensive and consistent application platform to develop, modernize, and deploy containerized and virtualized applications at scale, including modern AI-enabled applications.

Red Hat OpenShift AI

A platform for managing the lifecycle of predictive and generative AI models, at scale, across hybrid cloud environments.

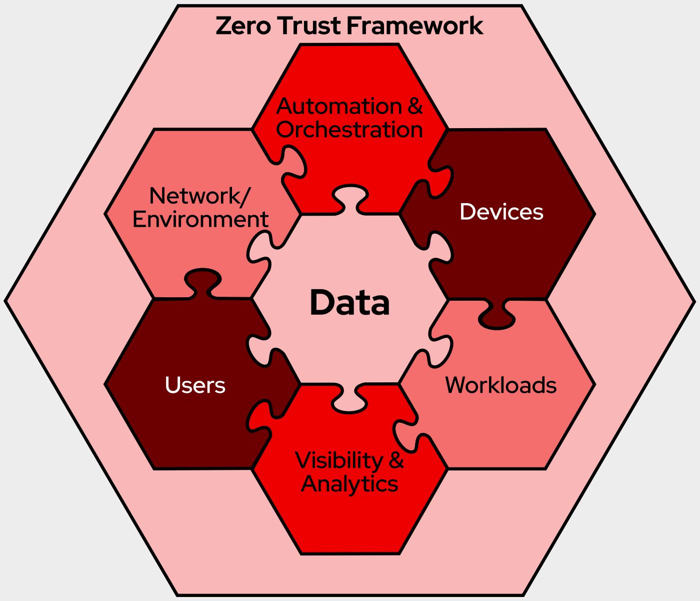


Figure 1. The 7 interlinked pillars in the DoD Zero Trust Reference Architecture

Enable defense

A hardened cyber terrain with reduced attack surfaces is more defendable and results in a better understanding of IT estates, as well as the implementation of visibility and security policy enforcement points. Both results provide an effective defense on traditional network perimeters within internal lateral movement pathways. The most valuable weapon any defender has is time—their own time to find and react to attack attempts, while forcing attackers to waste their own time in attempts to gain footholds, laterally move, and escalate privileges. The more visibility and enforcement points there are, the noisier attackers become, and the sooner both detection and mitigation can occur. Even as adversaries evolve their TTPs, the anatomy of attacks generally remains similar, and granular, pervasive visibility and control throughout a well-understood IT estate gives defenders a home field advantage.

For those organizations which build software, CORA assessments and defense should also extend into the software development lifecycle (SDLC) to ensure visibility and control points exist even in early software pipeline stages all the way through production deployment. These visibility and control points reveal what software contents are (Software Bill of Materials), and also cryptographically sign artifacts as they move through an SDLC to ensure that the contents of software are provably attested to and tied to developer identities. While the SDLC is not traditionally considered to be a focus for IT defense, modern adversaries are increasing attacks on software supply chains as well as AI code assistants to embed malicious code into mission software as early as possible to avoid detection and increase the depth and breadth of persistence across increasingly interconnected warfighting domains.

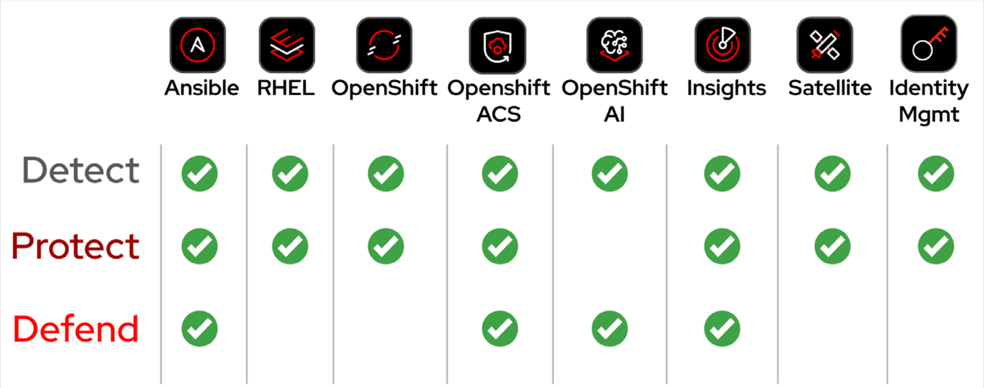
Ultimately, what CORA aims to achieve is a holistic and continuous risk-based cyber defense posture for enterprise and tactical DoD systems. The best defense is a good offense, and mapping the results of CORA assessments to DoD Zero Trust controls and frameworks shapes a traditional defensive posture into a more active posture that deliberately enforces identity-based policies throughout a system or system-of-systems. The Department of Defense Zero Trust Overlays[2] document published in June 2024 is an effective guide for this activity, mapping traditional NIST 800-53 controls into the current Zero Trust framework.

Red Hat portfolio alignment

The activities involved in performing a CORA assessment and continuous enforcement actions will lean on each system's component technologies to provide visibility and control points. A consistent platform implemented across both enterprise and tactical systems will reduce the friction of this effort and increase repeatability and standardization of both telemetry and security policies. Red Hat product portfolio provides this standardized, foundational infrastructure in the datacenter, public/private clouds, or on the mission edge on which applications can be developed, run, and iterated. Red Hat's portfolio of open source and open protocol products that are highly interoperable with other technologies in an IT estate, ensuring that a holistic and defensive posture is attainable.

- **Red Hat® Insights** collects and analyzes telemetry from the Red Hat portfolio and applications to reveal relevant security advisories, malware, CVEs, and compliance gaps to reliably predict risk, recommend actions, and provide automated remediation actions.
- **Red Hat Enterprise Linux®** in the datacenter, cloud, or on the mission edge, reports OpenSCAP STIG compliance, privilege escalations, terminal commands, SElinux events, application allowlist activity, and host-based firewall events to Insights and/or any log aggregation platform or Security Information and Event Management (SIEM).
- **Red Hat Satellite** contributes system cataloging, operating system, software inventory, and management telemetry.
- **Red Hat Ansible® Automation Platform** performs enterprise-wide interrogation of Windows and Linux systems, network devices, security appliances, storage devices, and more to collect a wide range of telemetry for developing mitigation plans.
- **Red Hat OpenShift® Container Platform** collects standardized, telemetry from containerized and virtualized workloads, and when paired with Red Hat Advanced Cluster Manager and Red Hat Advanced Cluster Security, also provides multicluster, application, network visibility, and control over containerized and virtualized applications through the entire software development lifecycle.
- **Red Hat OpenShift AI** develops, trains, and hosts on-premise and cloud artificial intelligence and machine learning (AI/ML) workloads used by CORA assessors to surface insights and anomalies from the entirety of telemetry collected from the IT estate under assessment. This flexibility of deployment options ensures that models are built and trained both where they are most relevant and where they are most protected.
- **Red Hat Build of Keycloak and Identity Management** contribute authN, authZ, and multifactor authentication (MFA) telemetry across Red Hat's portfolio and any other partner and third-party platform that supports Security Assertion Markup Language (SAML) or OpenID Connect (OIDC) authentication.

[2] *U.S. Department of Defense News. "New 'Overlays' Provide Guide on Path to Zero Trust." 4 June 2024.*



	Ansible	RHEL	OpenShift	Openshift ACS	OpenShift AI	Insights	Satellite	Identity Mgmt
Detect	✓	✓	✓	✓	✓	✓	✓	✓
Protect	✓	✓	✓	✓		✓	✓	✓
Defend	✓			✓	✓	✓		

Figure 2. Red Hat AI product portfolio capabilities align with DoD cybersecurity needs

Summary

Risk-focused continuous monitoring, assessment, and remediation are essential to counter the rapid evolution of modern adversaries. The nature of warfare develops rapidly across joint and coalition forces becoming more distributed, dynamic, and interconnected. This is an evolution that promises new and effective warfighting capabilities, but also presents new and nuanced attack surfaces for adversaries. As targeted threats grow in number and complexity, Red Hat assists the DoD in supporting the CORA framework to maintain decision dominance in the all-domain cyber battlespace.

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.

f facebook.com/redhatinc
𝕏 @RedHat
in 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