RAPID7

DATASHEET

STRENGTHENING COMPLIANCE WITH DOD'S CORA

ENHANCING VULNERABILITY CATEGORIZATION AND MITIGATION WITH RAPID7'S INSIGHTCLOUDSEC AND NEXPOSE SOLUTIONS

Introduction to CORA

The Cyber Operational Readiness Assessment (CORA), formerly known as the Command Cyber Readiness Inspection (CCRI), is led by the Defense Information Systems Agency (DISA) to evaluate and enhance the cybersecurity posture of Department of Defense (DoD) organization's networks, operating systems, and information assurance programs. It aims to identify vulnerabilities, enforce compliance with updated policies, and strengthen cyber readiness, ensuring high security standards and protecting critical DoD systems from cyber threats.

CORA Requirements for Government Agencies

The requirements of CORA mandate that government agencies, particularly those under the purview of the DoD, adhere to stringent cybersecurity standards. These standards encompass a broad spectrum of criteria, including robust network infrastructure defenses, compliance to updated security policies, rigorous incident response protocols, and comprehensive user training programs. Agencies must ensure continuous monitoring of their IT environments to promptly detect and mitigate vulnerabilities, thereby safeguarding sensitive information and maintaining operational integrity.

Understanding Vulnerability Categories

These vulnerability categories are used to classify the severity and potential impact of deficiencies within cybersecurity frameworks of the DoD.

- **CAT I vulnerabilities** are the most critical and severe. They represent weaknesses in cybersecurity defenses that, if exploited, could result in significant damage to national security, mission-critical systems, or sensitive information.
- **CAT II vulnerabilities** are less severe than CAT I but still pose a notable risk to organizational security. These vulnerabilities may expose systems or data to unauthorized access or compromise.
- **CAT III vulnerabilities** are considered moderate in severity. While they may not pose an immediate threat or have a significant impact on security, they still represent potential weaknesses that could be exploited under certain conditions.

These categorizations help organizations prioritize their vulnerability management efforts, allocate resources effectively, and maintain compliance with cybersecurity standards and regulations such as those outlined by CORA for government agencies.

HOW RAPID7 CAN HELP

Continuous Adherence to theMITRE ATT&CK Framework

Rapid7 supports customers in maintaining CORA compliance by enabling continuous alignment with industry standards across all resources. InsightCloudSec compliance packs address security, cost, and governance objectives, integrating frameworks such as FedRAMP, NIST, and AI/ML Best Practices. The MITRE ATT&CK Mitigation Pack aids organizations with over 300 compliance rules, focusing on benchmarking themselves against the tactics and techniques that span cloud and container environments.

Comprehensive Threat and Vulnerability Intelligence

Rapid7 is a Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA), authorizing the assignment of CVE numbers to vulnerabilities found in Rapid7's and any other vendors' products. Active Risk is Rapid7's built-in strategy for assessing and analyzing vulnerability risk on a scale of 0-1000. Active Risk uses the latest CVSS score with intelligence from threat feeds like AttackerKB, Metasploit, ExploitDB, Project Lorelei, CISA KEV list, and other third-party dark web sources to provide security teams with a threataware vulnerability risk score and to help prioritize remediation for the most critical vulnerabilities.

Identify Critical Exploitable Vulnerabilities

Moving beyond conventional vulnerability scanning, Rapid7 leverages the Metasploit Framework to conduct automated assessments that identify exploitable vulnerabilities posing the highest risks within networks.

Network Scanning

Rapid7 tools automate network and vulnerability scans with precision, ensuring thorough risk assessment across every facet of the attack surface. Customers can effortlessly configure robust authenticated scans with operating systems including various distributions of Linux, Windows, and Mac. Nexpose has the ability to perform authenticated scans on network devices (routers, switches, firewalls). Network devices have been a focus of Advanced Persistent Threats (APTs) targeting critical infrastructure to gain a foothold. This comprehensive approach enables detailed inspection of assets to uncover vulnerabilities and security policy violations beyond the capabilities of traditional network scanning tools.

Products Aligned with CORA

- **InsightCloudSec**: Fully-integrated cloudnative security platform
- **Nexpose**: On-premises option for vulnerability management software

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more or start a free trial, visit:
rapid7.com/try/insight