FedRAMP Updates ConMon!

Don't Let Your Monthly ConMon Subscriptions be Impacted

KRATOS

The FedRAMP PMO strongly encourages authorized cloud service providers to sign up for notifications of CISA catalog updates and remediate all the vulnerabilities it lists: Known Exploited Vulnerabilities Catalog Update Bulletin.

CISA will determine vulnerabilities warranting inclusion in the catalog based on reliable evidence that the vulnerability is being actively used to exploit public or private organizations by a threat actor.

NEWS

The Department of Homeland Security (DHS) Cybersecurity Infrastructure Security Agency (CISA) has issued Binding Operational Directive 22-0. FedRAMP PMO published guidance to reinforce the Directive's requirements. Kratos Continuous Monitoring Service (ConMon) can help you stay on top of the new requirements

FedRAMP Directive

The Directive establishes a CISA-managed catalog of exploited vulnerabilities that carry significant risk to the federal enterprise and establishes requirements for agencies to remediate any such vulnerabilities included in the catalog.

New FedRAMP Requirements

The catalog lists exploited vulnerabilities that carry significant risk to the federal enterprise and requires that they be remediated within six months for vulnerabilities with a Common vulnerabilities and Exposures (CVE) ID assigned prior to 2021 and within two weeks for all other vulnerabilities.

POA&M Template Update

FedRAMP has updated the POA&M template to accommodate tracking of vulnerabilities against the catalog of known exploited vulnerabilities. The new 'Binding Operational Directive 22-01 tracking' column should be filled out with a 'Yes' or 'No' as to whether this POA&M item's vulnerability is found in the catalog of known exploited vulnerabilities.

Non-compliance Penalties

Escalation for any late item will be handled by the JAB with a Detailed Finding Review (DFR) or Corrective Action Plan (CAP) based on the individual vulnerability. Since CISA requires timely remediation for these vulnerabilities, organizations will not be permitted to submit deviation requests.

Compromise Indicators

If any indication of compromise or anomalous behavior is found or there is any suspected impact to federal systems, please make sure to follow the FedRAMP Incident Communication Procedures, which includes reporting to:

- CISA US-CERT,
- Agency customers, and
- FedRAMP JAB POCs.

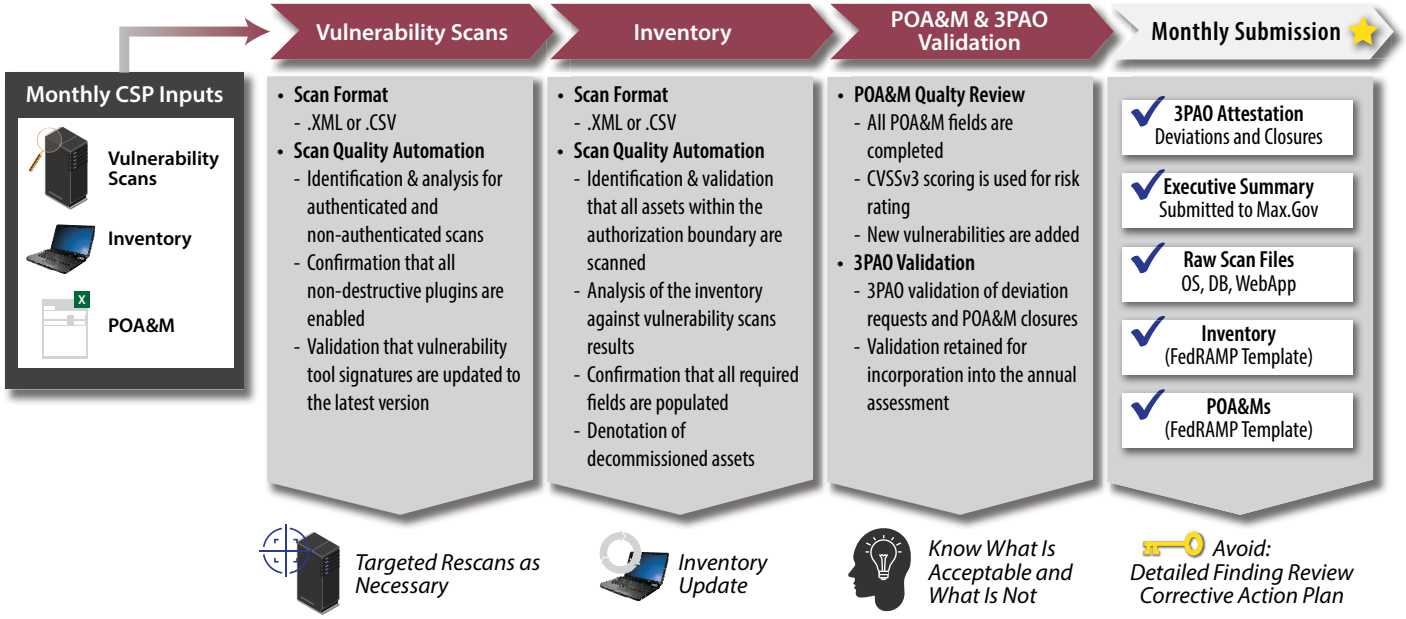
ONLINE RESOURCES

- Binding Operational Directive 22-01
- CISA Known Exploited Vulnerabilities Catalog
- Plan of Action and Milestones (POA&M) Template Completion Guide
- FedRAMP Plan of Action and Milestones (PO&AM)Template

Phone: 703-254-2016 • EMail: CyberSales@KratosDefense.com • Web: www.KratosDefense.com

ConMon Services

Kratos provides ConMon advisory and assessment services to customers to support the management and quality submissions of FedRAMP required inventories, vulnerability scans, POA&Ms, deviation requests and more. These services help Cloud Service Providers (CSPs) maintain their ATO. Kratos provides on-going continuous monitoring services on a quarterly, annual, or every



three- or five-year basis to satisfy FedRAMP requirements.
Kratos services include the mandatory services to be performed by a 3PAO on an annual basis, such as:

- Assessing a subset of controls
- Performing penetration testing
- Scanning operating systems/infrastructure, web applications, and databases
- Assisting in CSP self-attestation, change control, and incident response reporting

Why Kratos ConMon Services?

- Maintain and simplify compliance on an ongoing basis
- Access real-time views of risk versus "point-in-time" legacy risk methods
- Automate manual tasks to reduce time and resource constraints
- Remediate issues proactively
- Attest to compliance with greater accuracy
- Significantly reduce vulnerability exploitation time windows

Contact US:

If you have any questions about the FedRAMP updates or would like to know more about our ConMon services, contact us at:

CyberSales@KratosDefense.com.