DOMENIX
Relevant Technology

Chemical, Biological, Radiological, and Nuclear Common Operating Repository (CBRN CORe)

In support of the Defense Threat Reduction Agency (DTRA) RD-CBI, Domenix provides a centralized repository, "CORe" for software applications, code, and associated data sets and containerization and hardening in accordance with DISA guidelines that will serve as the foundation of a Digital Laboratory and enable AI/ML capabilities..

CBRN CORe provides a Development, Security, and Operations (DevSecOps) Continuous Delivery Continuous Integration (CI/CD) capability for the consistent and reproducible collection, organization, shared library management, assessment, sustainment, and transition of the enterprise software and data inventory.

CBRN CORe is an enterprise DevSecOps Software Factory that provides all key components necessary for consistent configuration managed development, evaluation, maturation, and positioning for the deployment of software (i.e., source code, firmware, data sets, common components, AI/ML capabilities, containers, plug-ins, algorithms, visualizations, and associated documentation). Domenix is collecting a variety of diverse Windows, Linux, and handheld software and data sets from various providers and performers from DTRA in-house and external developers. For each, we use a common set of project and issue templates tailorable CI/CD pipelines, governance, and business rules to:

- **Organize the software in projects**, using project templates to standardize the organization, format, and presentation of all items in the inventory format so all items in the inventory have a common look and feel and Wikis detailing key aspects of maturity, run-time and deployment specifications, and information safeguarding and dissemination requirements.
- **Segregate the software** into Impact Levels (IL) 2, 4, and 5 "boundaries" utilizing combinations and configuration of Group and Role Based Access Permissions (RBAC) and MFA (user name, password and authenticator apps) and MFA (CAC/PIV) smart-card authentication.
- **Instantiate the software into a CI/CD pipeline** based on DISA requirements, such that the automated process of building and scanning is uniform across the entire inventory.
- **Assess the software** in terms of its maturity, independent reproducibility (from source code), and the robustness of its documentation and determine whether the component should be a shared component or library to be utilized across multiple projects.
- **Scan the software** using DISA approved scanning tools and provide results to performers to resolve vulnerabilities to "harden" the software.
- **Containerize and Harden the software** where appropriate. DISA provides guides for Linux. DISA support for Windows containerization and hardening continues to evolve. For handhelds, we position those apps and plugins to meet requirements of DoD approved app storefronts.
- **Host the software in a secure AWS GovCloud environment** that allows the entire environment to be portable to other FedRAMP Authorized providers (e.g., Microsoft Azure) or other government or DoD cloud environment (DISA Stratus) with no vendor lock-in.

Why CORe?

To provide a DoD Joint DevSecOps Software Factory for DTRA. Allows Joint, Service-Specific, non-DoD (including academia and not-for-profits) to participate in a common environment to develop, mature, and transition software. CORe provides the ability to extend the pipelines to target specific host platforms and provides a foundation for a Digital Laboratory to apply advanced AI/ML and immersive virtual reality technologies to address complex CBRN problems in a holistic way.

DOMENIX
Relevant Technology

Enterprise US Chemical Biological Defense Program (CBDP) Joint DevSecOps

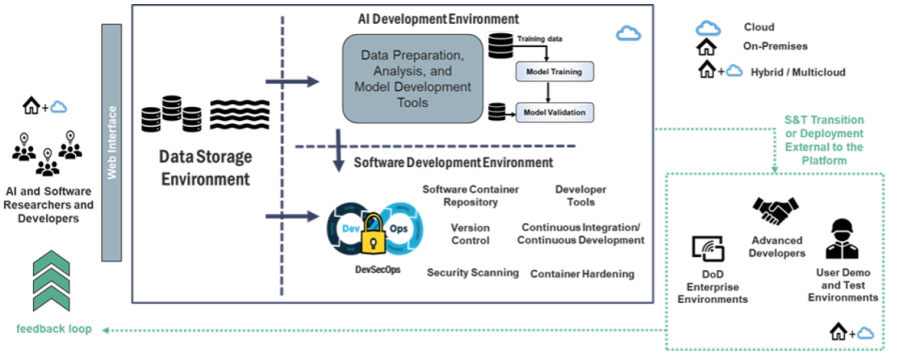
CORe is driving CBDP development with the following motivations and goals in mind:::

- **Improved organization and consistency of knowledge** about the system – Leading to better informed and more rapid decision making.
- **Enhanced consistency and efficiency of data** integration among disciplines – leading to better engineered systems and system-of-system integration.
- **Systems that better meet mission needs** to enable early and frequent verification of requirement/design closure.
- **Provides early warning of disconnects** to reduce risk of costly redesign schedule setbacks.
- **Early discovery and mitigation of SE problems** to examine completeness and consistency of the design at every stage.
- **Reduces the risk of propagating inconsistencies** to provide a means of identifying a needed focus for unresolved design aspects and to improve lower-level design closure with system-level design.
- **Improved rationale and validation** to enable traceability amongst all related system artifacts throughout its life cycle.

CORe Project Management

The shift-left movement in DevSecOps development makes integration security considerations essential to every development iteration and sprint. DevSecOps is the addition of security considerations and practices to an organization's CI/CD workflow.

CORe Vision: A Digital Laboratory: Unified DevSecOps Software Factory, AI/ML and Big Data Platform



DevSecOps, spans development, cybersecurity, QA testing, IT operations and support teams

CORe Insights:

- **Hosted in a (US) Virtual Private Cloud** (VPC). The CORe VPC consists primarily of a CORe Host Platform (CHP) plus Linux and Windows servers that support assessment, prototyping, development, integration, testing, and evaluation.
- **Supports IL2, IL4, and IL5** and is planning for an IL6 instantiation in the near future.
- **Uses GitLab Ultimate** to manage and execute CORe, utilizing the Agile methodology.
- **Improves understanding** of composition and capabilities of the CBRND enterprise.
- **Identifies interdependencies** among components of the enterprise.
- **Integrates knowledge** across the enterprise, reducing stovepipes and duplication of effort.
- **Increases standardization** and integration at the system level.
- **Provides integrated data science, AI/ML**, and software development functions within a consolidated development, security, and operations (DevSecOps) environment.

What's Next?

Connect with us to schedule a live CORe demo. Hear how CORe can establish an integrated digital approach that uses authoritative sources of system data and models as a continuum across disciplines to support life cycle activities.

Phone : (571) 278-5400 | **Email :** contactus@Domenix.com
Address : 4229 Lafayette Center Drive, Suite 1800 Chantilly, VA 20151

www.Domenix.com