Cyber Testing for Resilient Industrial Control Systems™ (CyTRICS)

The Department of Energy's program for cybersecurity vulnerability testing, forensic analysis, and subcomponent enumeration.

CyTRICS enhances the cyber resilience of highly critical equipment in the energy sector by partnering with stakeholders to identify high priority operational technology (OT) components/systems, perform expert testing, share information about vulnerabilities in the supply chain, and inform improvements in component design and manufacturing.

CyTRICS was developed to address growing concerns that adversaries could exploit weaknesses in digital supply chains, possibly triggering catastrophic effects on energy infrastructure and beyond. Accordingly, CyTRICS applies threat intelligence, identifies common mode vulnerabilities in high-impact hardware, software, and firmware and responsibly discloses them to manufacturers and asset owners, who can act to address these weaknesses before they can be exploited.

CyTRICS leverages best-in-class test facilities and analytic capabilities from multiple DOE National Laboratories and strategic partnerships with technology developers, manufacturers, asset owners and operators, and interagency partners.

CyTRICS integrates several innovative processes:

Prioritization Methodology: A transparent approach to prioritizing test operations that scores OT components/systems across key factors such as operational impact, prevalence, and other technical characteristics. The methodology also weights national security interest to maximize the impact of testing.

Testing Process: A refined, standardized approach to vulnerability testing and subcomponent enumeration for hardware, software, and firmware. Standardization ensures consistency, repeatability, and comparability of results, enabling scale up of testing beyond DOE National Laboratories to industry partners.

Partner Agreements: Formal participation agreements executed with top manufacturers and asset owners to frame cooperation and supply components/systems for testing. The standard agreement establishes the scope of testing and a process for responsibly disclosing vulnerability information.

Data Repository: A central data repository that stores bills of materials (BOMs or "digital lists of ingredients") from testing for cross-component and impact analysis. The repository enables rapid identification of high-risk subcomponents and sector-wide analysis of systemic risks and vulnerabilities.

Conceived in 2018, CyTRICS completed proof-of-concept testing and used these results to develop a standardized testing process, results reporting formats, and a data repository in 2019. CyTRICS then validated core program processes through pilot testing in 2020 and achieved initial operating capability in 2021. The program will achieve full operating capability in late 2022 and begin evolving into a national center of excellence in 2023.

CyTRICS vulnerability testing and subcomponent enumeration aligns with multiple DOE cybersecurity initiatives. CyTRICS leverages the Securing Energy Infrastructure Executive Task Force (per § 5726, FY20 NDAA) for strategic and technical engagement with Energy Sector Industrial Base partners in the design, implementation, and operation of the program; CyTRICS solicits feedback to continuously refine program processes – prioritization, testing, analytics, and vulnerability disclosure – to reflect industry best practices and evolving policy. CyTRICS is also the central component of the new Energy Cyber Sense program (per § 40122, FY22 Infrastructure Investment and Jobs Act), which integrates DOE cyber supply chain programs.

For more information, visit the CyTRICS website: https://inl.gov/cytrics/