Encrypt Sensitive Information, Mitigation M0941 - ICS

By Authorization Enforcement

Archived: 2026-04-05 16:17:10 UTC

Domain	ID	Name	Use
ICS	T0811	Data from Information Repositories	Information which is sensitive to the operation and architecture of the process environment may be encrypted to ensure confidentiality and restrict access to only those who need to know. [1] [2]
ICS	T0893	Data from Local System	Information which is sensitive to the operation and architecture of the process environment may be encrypted to ensure confidentiality and restrict access to only those who need to know. [1] [2]
ICS	T0839	Module Firmware	The encryption of firmware should be considered to prevent adversaries from identifying possible vulnerabilities within the firmware.
ICS	T0873	Project File Infection	When at rest, project files should be encrypted to prevent unauthorized changes. [2]
ICS	T0857	System Firmware	The encryption of firmware should be considered to prevent adversaries from identifying possible vulnerabilities within the firmware.
ICS	T0882	Theft of Operational Information	Encrypt any operational data with strong confidentiality requirements, including organizational trade-secrets, recipes, and other intellectual property (IP).
ICS	T0864	Transient Cyber Asset	Consider implementing full disk encryption, especially if engineering workstations are transient assets that are more likely

Domain	ID	Name	Use
			to be lost, stolen, or tampered with. [2]

Source: https://attack.mitre.org/mitigations/M0941