Certificated connectivity triggers for controlled access windows

Name Invisibility Cloaking Mode

Application Mislead attackers from behind a canary

Sectors Enterprise, Utility, CNI, Defense

Description Configured to present a public interface to a canary endpoint for the majority of the time. Ensures enumeration and attacks gain no leverage. As controlled on schedule or access window by SIEM or similar, the active physical interface is switched to the high value asset. At all times the emergency physical closure of access can be revoked rapidly.

Typically used to hide highest value assets behind an innocuous service that acts as a canary and obfuscates real asset enumeration and attack.

Hide-Unhide Controller

SIEM – Access Grant / Scheduler

External Zone

FireBreak 1

Firewall

CANARY DEVICE — A

FireBreak 2

Firewall

High Value Asset — B

goldilock