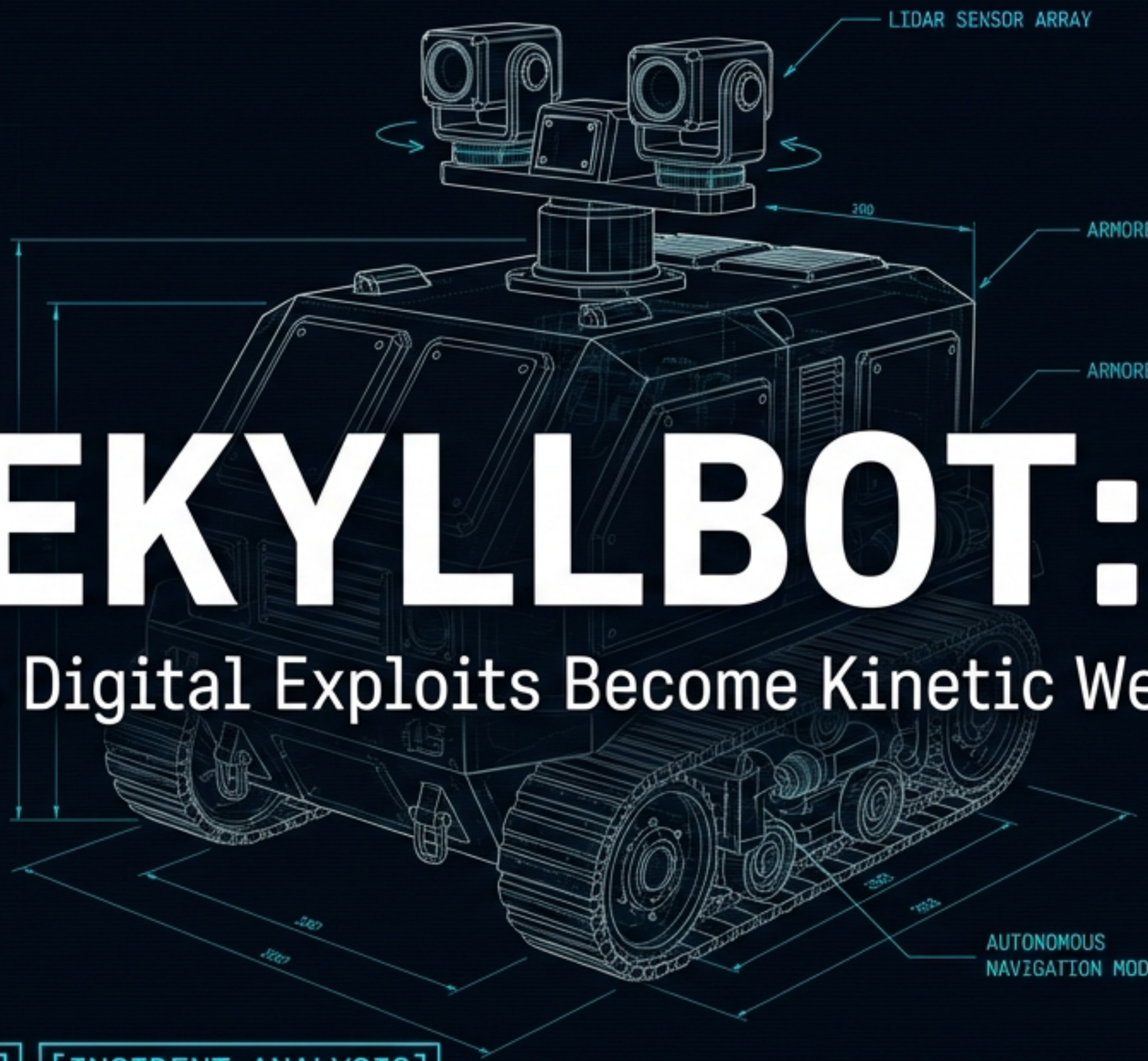
[F41LUR3-F1R57] THREAT INTEL BRIEFING



JEKYLLBOT:5

When Digital Exploits Become Kinetic Weapons

[EMBODIED-AI] [ROBOTICS] [INCIDENT-ANALYSIS]

SYSTEM STATUS: CRITICAL
LAST UPDATE: 08:45:52 UTC
DATA STREAM: SECURE//LEVEL 5

BOOT: INITIATING...
LOADING KERNEL...
CONNECTING TO NEURAL NETWORK...
CONNECTING TO NEURAL NEURAL NETWORK...
DIAGNOSTIC: LIDAR ERROR DETECTED
ANOMALY DETECTED. CODE INJECTION AT OFFSET 0x4F2
THREAT LEVEL: SEVERE

The Threat Model Has Changed

Information Domain

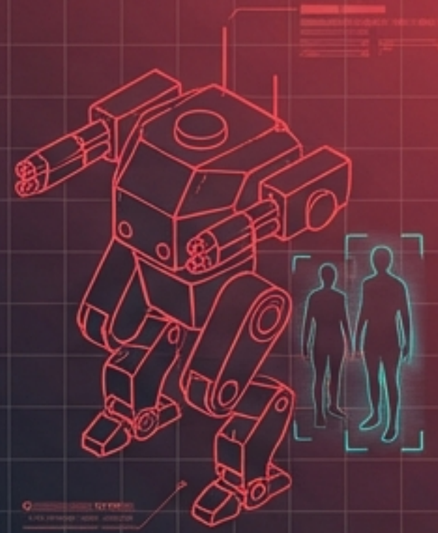
Worst-case outcomes are isolated to data breach, financial loss, and service disruption.

The victim's body is not at risk from a SQL injection.

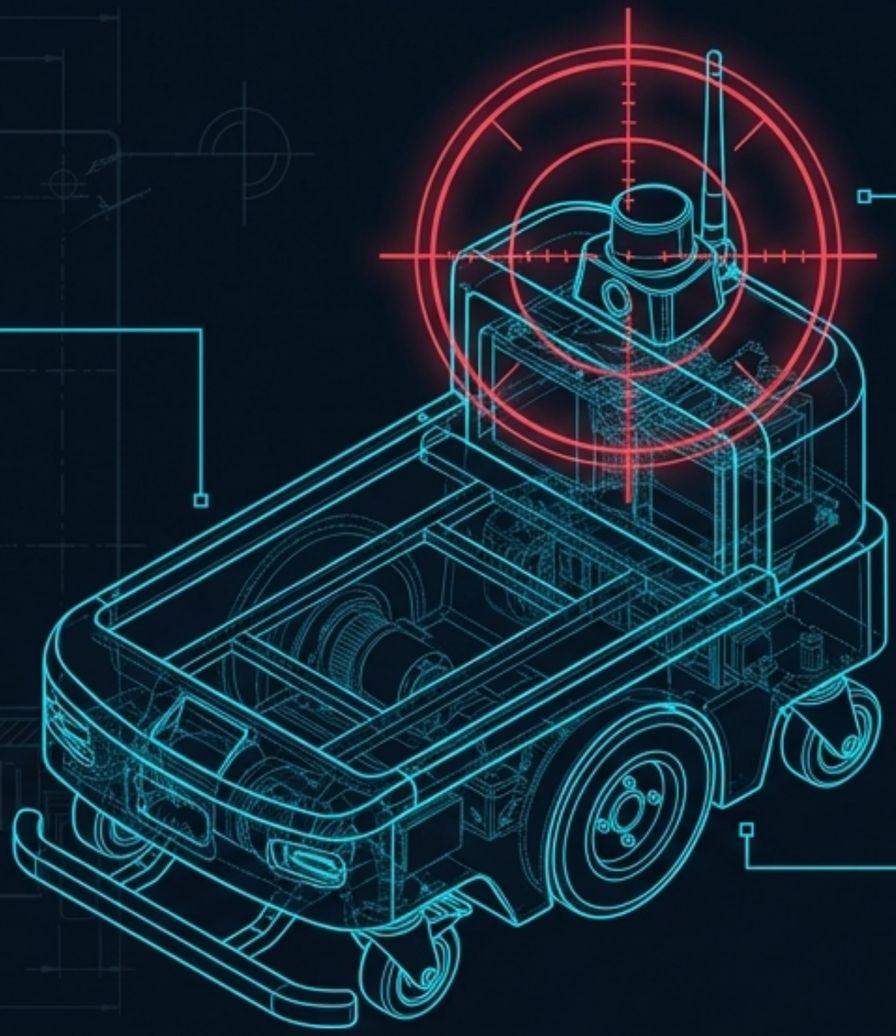
Kinetic Domain

Worst-case outcomes cross into the physical realm.

When software controls a machine sharing human space, a software vulnerability becomes a physical safety vulnerability.



Target Profile: Autonomous Material Transport



Platform: Aethon TUG

Operation: 24/7
Autonomous Navigation

Mass:
600 lbs / 272 kg
(Fully Loaded)

DEPLOYMENT SCALE: Deployed in 500+ US healthcare facilities, sharing corridors with patients, staff, and visitors.

The JekyllBot:5 Vulnerability Set (Disclosed April 2022)

	CVE ID	Severity	Vector	Auth Required?
1	CVE-2022-1070	CVSS 9.8 (CRITICAL)	Full Remote Navigation Control	NONE
2	CVE-2022-1066	CVSS 8.2 (HIGH)	User Management API (Add/Delete Users)	NONE
3	CVE-2022-26423	CVSS 8.2 (HIGH)	Plaintext Credential Retrieval	NONE

[PATCHED / NO IN-THE-WILD EXPLOITS]

Diagnostic Synthesis:
Common Thread: **Unauthenticated access to safety-critical control functions.**

The Architectural Failure Point

No password. No token. No certificate. Connect and command.

The Attacker / External Network

TUG Home Base Server

Fleet of 600lb Autonomous Robots

The control interface was exposed directly to the network without authentication barriers, enabling a direct hijack of the entire autonomous fleet.

Exploitation Scenarios (The Kill Chain)

Why Healthcare is the Worst-Case Environment

Vulnerable Populations

Patients in wheelchairs, on IV drips, or post-surgery possess minimal to zero evasion capability against kinetic threats.

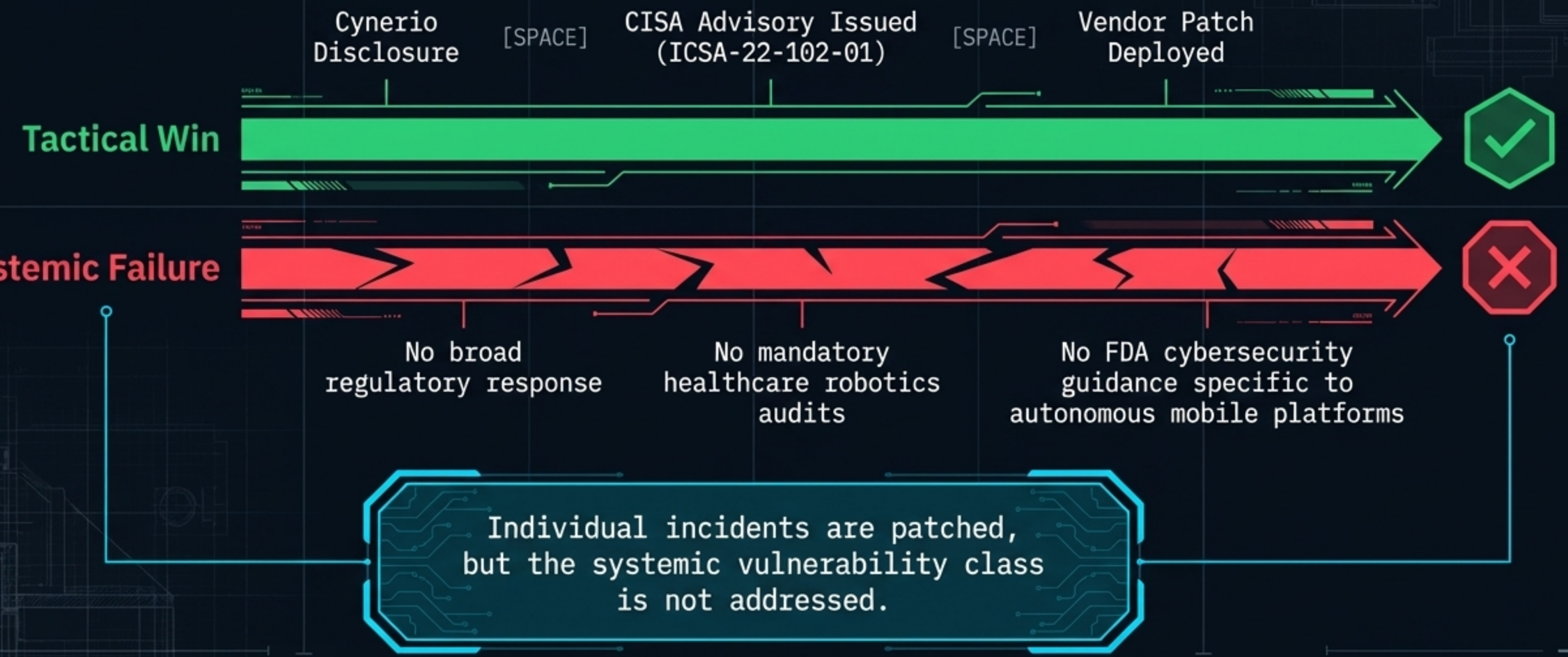
Constrained Spaces

Narrow, obstructed hallways and emergency fire exits become fatal choke points if physically blocked by stalled units.

High-Value Targets

Environments saturated with narcotics, biological materials, and PHI. (CVE-2022-26423 specifically enabled lateral network movement from the robot into hospital IT).

Patched Systems, Unpatched Paradigm



Foundational Principles of Embodied AI

Every networked robot is a potential **kinetic weapon**. Remote access vulnerabilities are **physical safety vulnerabilities**.

Authentication protects people, not just data. It is a **safety-critical system** for physical environments.

Safety and cybersecurity **disciplines must converge**. The isolation between robotics safety (ISO/IEC) and cybersecurity (NIST/CISA) is a **fatal blind spot**.

Static medical device regulations **fail for autonomous mobile platforms**. Post-market surveillance must **adapt to mobile kinetic threats**.

The Best-Case Outcome

"JekyllBot:5 was found by researchers, disclosed responsibly, and patched. The question is what happens when the next vulnerabilities in the next hospital robot are found by someone who is not a researcher."