MirrorMire
PROACTIVE CYBER RESILIENCE

Detect, Engage, and Divert adversaries before they reach your critical assets.

Unified proactive resilience across OT, IT, Identity and AI environments.

Where Reactive Security Falls Short

Attackers move quietly across OT, IT, and AI environments, while most security tools monitor each environment separately and respond only after suspicious activity has already been detected. In operational environments, that delay matters. OT cannot be secured exactly like IT, and intrusions are often discovered late, or not at all.

Proactive Security Outcomes

- ✓ Detect intrusions earlier in the attack path
- ✓ High-confidence alerts
- ✓ Deploys without agents or changes to live controllers
- ✓ One unified view: OT, IT, Identity, & AI
- ✓ Faster incident response
- ✓ Audit-ready reporting

How Mirrormire Works

1

Map

(Real-Time Threat Profiling)

Profiles attacker behavior in real time, identifying intent, tracking movement patterns, and predicting attack paths before they reach critical systems.

2

Maneuver

(Autonomous Threat Redirection)

Actively redirects adversaries away from sensitive infrastructure into high-interaction synthetic environments, increasing attacker engagement time and reducing harm to real assets.

3

Maze

(Intelligence-Driven Defense and Response)

Captures attacker TTPs, extracts malware and behavioral data, and feeds actionable intelligence into your existing security stack (e.g. SIEM/SOAR) for immediate response.

The AMaze™ Platform

Synthetic Cognitive Agents

AI-Native advanced decoys that mimic high-value assets, luring and trapping attackers in realistic mirrored environments.

Real-Time TTP Extraction

Captures full attacker Tactics, Techniques & Procedures inside isolated mirrored environments.

Automated Response Integration

Feeds live intelligence into SIEM, SOAR, WAF, and Micro-Segmentation tools for instant automated blocking/SOC, human in the loop.

AI Agent Security

Deploy AI SCAs anywhere your AI lives. drop-in MCP honey-server, LLM proxy/sidecar alongside your IT and OT defenses.

Neural Echoes (Zero False Positives)

Advanced dynamic lures redirect adversaries from real assets into synthetic environments producing high fidelity alerts.

Malware / Ransomware Capture

Captures and analyzes malware dropped by adversaries thus preventing damage to real systems.

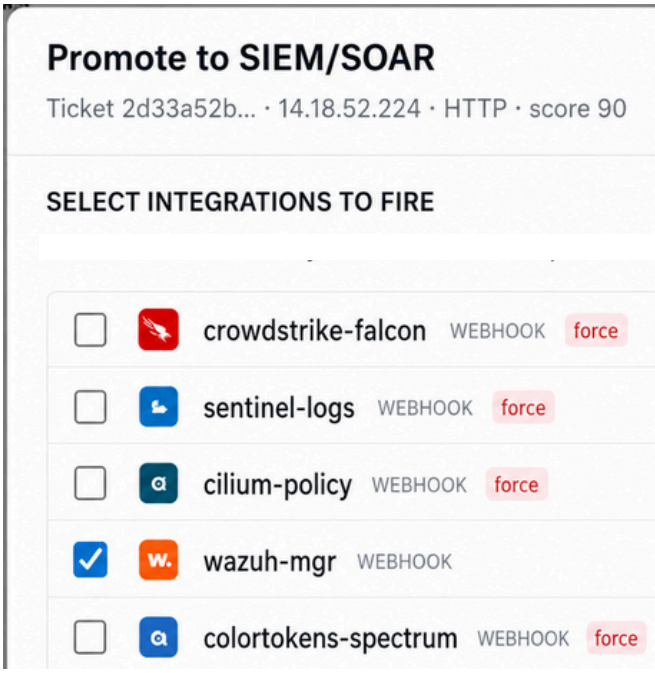
Unified IT/OT Protection

Seamless defense across IT, OT, and transition zones, securing the messy middle attacker's exploit.

The AMaze™ Ecosystem

When AMaze™ confirms attacker activity, you do not receive another context-free alert. You receive a ready-to-investigate event with the source IP, threat score, protocol, and mapped MITRE ATT&CK techniques already attached.

Through a strategic cybersecurity partnership, AMaze™ is currently being rolled out across more than 80 operational energy plants in the United States, bringing deception-based protection to real-world OT and IT environments without disrupting production systems.



Ready to see AMaze™ in action?

Contact our team to book a demo or learn more

info@mirrormire.ai