ILLUSIVE PLATFORM FEATURE BRIEF:

IoT Emulations

40 billion IoT devices will connect to the internet by 2025, each one a juicy target awaiting attacker exploitation. The impossibility of effectively patching or monitoring IoT devices, along with their sheer diversity, creates a mass of ideal network locations for attackers to carry out reconnaissance, surveillance and data theft undetected. Deploy protection to safeguard these otherwise unsecurable devices before attackers can take advantage. Illusive IoT Emulations poison your potential attack surface by flooding your network with a scalable web of deceptive IoT devices that appear real to attackers. The emulations send a high-fidelity incident record to defenders upon attacker interaction, with full and detailed forensics, so your organization can respond to and block IoT threats in real time.

BENEFITS

- Frictionless, high-fidelity IoT device attack detection and intelligence
- Shut down attackers seeking to prolong dwell time on otherwise unsecurable IoT infrastructure
- Customized emulations of any IoT device running on any IoT protocol
- Blanket your network with thousands of deceptive IoT devices in seconds

Detect IoT Attacks

Respond to IoT Attacks

Deceptive emulations blanketing your network and servers are indistinguishable from genuine IoT devices. They fool attackers into interacting with them and revealing their presence.

Illusive IoT forensics supply detailed information about attack methods, lateral movement, and affected systems, which can then be leveraged by third-party incident response systems to isolate or quarantine the threat.

How IoT Deceptions Work

1. Choose the IoT device emulations your organization would like to deploy from the Illusive catalog of preconfigured and tailor-made options
2. Distribute emulations of IoT devices and breadcrumbs leading to them throughout your servers, networks and endpoints
3. Attackers seeking to use IoT devices on your network can't tell real IoT devices from fake; disoriented, they inevitably interact with with the emulations
4. Upon engaging the deceptive IoT device, an incident report is sent to the organization with forensics on the attacker and their methods