ILLUSIVE PLATFORM FEATURE BRIEF:

OT Emulations

As IT security hardens and threats evolve, operational technology and industrial control systems are increasingly targeted: Stuxnet, TRITON, and the notorious attacks on Ukraine's power grid all illustrate the risks of vulnerable OT. These systems were designed decades ago without today's attacks in mind, and often can't be patched, monitored or protected with the latest controls. Air gaps meant to separate OT systems from IT infrastructure have already been compromised to enable successful attacks and are becoming untenable as the digital transformation compels changes to how companies do business. Illusive OT Emulations prevent attackers from reaching critical systems that can't be properly secured any other way. Through customizable deceptive emulations of your OT, Illusive forces attackers to reveal their presence so that essential infrastructure can continue to operate safely.

BENEFITS

- Eliminate threat detection blind spots in formerly unsecurable OT/ICS environments
- Proactively detect new and previously unseen attacks with no need to rely on previous attack signatures
- Actionable reporting that speeds up incident investigations and simplifies attack response
- Frictionless deployment with no infrastructure interruptions or need to take OT offline

Secure the Supposedly Unsecurable

Advanced OT emulations, as well as deceptive jump servers and workstations leading to them, appear to attackers like components of your real system. Attacker interaction with the emulations generates full forensics, enabling you to immediately stop in-progress attacks.

Economic and Effective OT Security

Critical OT infrastructure can't be taken offline without incurring heavy costs or serious societal interruptions. Efficiently and actively defend OT without the need to disrupt critical systems.

How OT Deceptions Work

1. Illusive works with an organization to create and distribute deceptive emulations of OT environment infrastructure on a network
2. An attacker seeking unauthorized access to an OT environment is tricked into interacting with an emulation instead of the real thing
3. As soon as the attacker accesses the OT emulation an alert is sent to the organization with full forensic evidence of the attacker's presence
4. The attacker is interrupted early in the attack lifecycle as the organization uses the intelligence Illusive collects to quickly respond