ILLUSIVE PLATFORM FEATURE BRIEF:

Deceptive Microsoft Office Beacon Files

Illusive's Deceptive Microsoft Office Beacon Files allow organizations to stop both malicious insiders and external attackers. Organizations can automate the creation and customization of hundreds of thousands of deceptive Word and Excel documents that are indistinguishable from the genuine article, right down to the usage of company logos and letterhead. These fake but seemingly real Office documents can be loaded with fake data that sets off an alert as soon as an attacker tries to use the information to gain access. In addition, both real and deceptive Word and Excel documents can be beaconized to immediately alert organizations to the presence of malicious insiders or external attackers as soon as they interact with whichever document you choose to protect.

BENEFITS

- Surgically identify insider threats with high fidelity
- Easily deploy and customize deceptive Word & Excel files indistinguishable from the genuine article at scale
- Turn any real or deceptive Word and Excel file into a beacon for early insider and attacker detection
- Fill deceptive Office documents with fake information that sets off an alert if used by an attacker to attempt access

Detect & Stop:

INSIDERS

Beaconized Office files, both real and deceptive, send off an alert upon interaction. This gives your organization the intelligence it needs to ID insiders and take action to stop them.

Detect & Stop:

INTRUDERS

Deceptive Office files can be customized to look like the real thing, but with fake data. Organizations are instantly alerted once attackers try to use the fake data to gain access to an account.

How Deceptive Microsoft Office Beacon Files Work

1. Illusive automates creation and distribution of fake Office files that look real, and beacons for both fake and real documents.
2. Attacker unknowingly accesses a highly authentic Office deception or a beaconized genuine document.
3. As soon as a beaconized document is accessed, or deceptive data in a fake doc is used to attempt access, organizations are alerted.
4. Organizations now have high-fidelity info about an intruder or malicious insider attempting unauthorized document access and can quickly respond.