DECEPTIONGRID™

AN ADVANCED CYBER-DECEPTION PLATFORM ABLE TO DEFEAT SOPHISTICATED ATTACKS WITH NO CHANGES TO THE NETWORK

Attackers only needs to find one weakness while defenders need to find and address every single one. This built in imbalance puts security teams at a disadvantage when trying to protect the modern enterprise spanning cloud, data center, campuses and IoT devices.

By feeding attackers misinformation we take away their ability to know what is fake and what is real and proceed with the attack.

TrapX DeceptionGrid™ changes the dynamic of cybercrime by diverting attackers away from real assets with a shadow network compromised of fake assets. The powerful security technology takes a three-pronged approach: deceive, detect, and defeat.

DeceptionGrid is agentless, requires no changes to the network and signature agnostic.

TRAPX DECOYS, ENGAGES, AND TRAPS ATTACKERS THROUGHOUT THE ENTIRE NETWORK

Deception technology provides wide-reaching cybersecurity at the lowest possible cost. The platform passively works with the network and other security measures to contain attacks and enable a return to normal operations.

When attackers penetrate an enterprise, they perform reconnaissance to recognize assets. DeceptionGrid traps appear identical in every way to real operational IT assets and connected Internet of Things (IoT) devices. A single touch of a decoy alerts cybersecurity teams of a potential attack.

BENEFITS

• Deception technology finds sophisticated attackers that may be present and undiscovered by traditional cybersecurity solutions.

• Extremely low TCO and fast time to value (easy and quick to deploy, no false positives, minimum ongoing operational burden)

• A multi-tier architecture enables better detection, deeper attacker engagement, and comprehensive containment.

• The DeceptionGrid passively integrates itself with existing operations and other vendor solutions already in place.

• TrapX alerts are over 99% accurate and provide immediate cyber threat detection, response, and intervention.

FEATURES

• Powerful emulation camouflages traps as any attack surfaces with out of the box templates for industry-specific items such as medical devices, POS terminals, SCADA, ATMs, and more.

• Highly scalable - each appliance supports 500 traps, requiring few resources even for largest Enterprise wide deployments

• End-to-end integration with existing solutions, automatically translating intelligence to mitigation

• Detailed Forensics and threat intelligence allowing you to know the mind of the attacker and disposition alerts swiftly and decisively

• Build Your Own Trap (BYOT) enables users to create fake attack surfaces and apps tailor-fit for environments or devices.

• Dynamic Deception enables artifacts to continuously shift to create a moving minefield that attackers cannot avoid.

• The DeceptionNet network allows users to share counter-measures and share of traps made by other community members.